State of California

Franchise Tax Board

E-Commerce Portal Infrastructure (EPI)

Feasibility Study Report

FTB FSR 06-01

11/28/06 Revision

Table of Contents

1.0 Executive Project Approval Transmittal

See Attachment 1.

2.0 Project Summary Package

See Attachment 2.

3.0 Business Case

3.1 Business Program Background

The Franchise Tax Board (FTB) serves the public by collecting tax revenues and operating other non-tax programs at the least cost while continually improving the quality of its products and services, warranting the highest degree of public confidence in its integrity, efficiency and fairness. The department administers the Personal Income Tax Law, the Bank and Corporation Tax Law, and the Homeowner's and Renter's Assistance programs. FTB also performs audits pursuant to the Political Reform Act; collects vehicle registration fees and other debts as authorized or required by the Legislature; and settles civil tax disputes that are the subject of protest, appeals, or refund claims.

As part of FTB's strategic plan, the *Filing 2010: The Future of State Income Tax Filing* document was prepared in 1996 and updated in 2000. This document describes a tax filing and information-processing environment significantly different from the traditional paper-processing environment. The *California State Information Technology Strategic Plan* further directs a shift from traditional paper processing to electronic services, or "e-commerce."

FTB has responded by using Information Technology to transform the way it does business. By 2005, FTB's e-file programs processed more than half of California's 14.5 million Personal Income Tax (PIT) returns. FTB's mission critical e-file and other e-commerce applications rely heavily on FTB's Internet infrastructure.

Research shows that citizens interacting with government who use e-commerce are more satisfied than those served by traditional means. Citizens using e-commerce feel that government is more responsive to their needs[1]. E-commerce also increases an organization's operational efficiencies while reducing long-term costs. An integral part of an organization's ability to provide e-commerce is its Internet infrastructure, which supports the e-commerce services that the public has come to expect from the private sector and now demands from government.

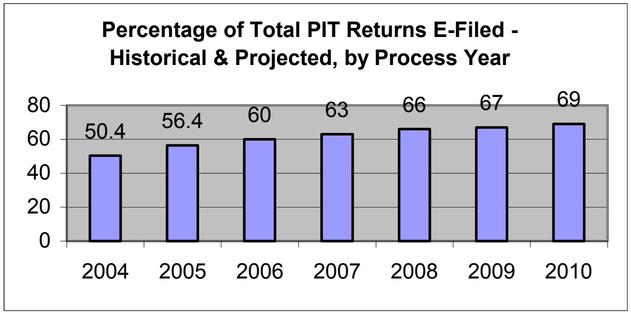
FTB's key business strategy is to leverage the current momentum in growth of the public's use of e-commerce and transfer more taxpayers to its e-commerce portal as the preferred method of interaction. FTB believes that, over the long-term, providing reliable e-commerce that is available 24x7x365 empowers taxpayers and their representatives to take more control of their interaction with government. This empowerment leads to an increased sense of cooperation between FTB and its customers, promotes self-compliance with tax law, and increases FTB's ability to accomplish its primary mission of efficiently collecting the appropriate amount of tax.

[1] **"E-Government: To Connect, Protect, and Serve Us,"** Hart-Teeter for the Council for Excellence in Government, 2002.

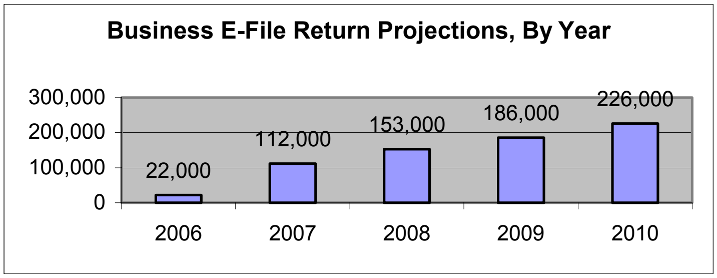
Over the past decade, FTB has seen a significant increase in the public's use and acceptance of e-commerce through FTB's Internet portal, including those services focused on compliance. As the private sector and leading agencies in the public sector have learned, e-commerce is no longer a secondary, optional means of customer service. FTB's e-commerce portal is now a primary business channel for meeting public demand for convenient, relevant services.

Over the years, FTB has increasingly encouraged its strategic business partners, such as tax practitioners, software developers, and other governmental agencies to use and rely on FTB's Internet for exchanging and obtaining information. Internet unavailability and vulnerability puts FTB's credibility at risk with its business partners it has encouraged or required to conduct business with FTB via the Internet, as well as putting the credibility of its business partners at risk with its customers. This has the potential of impacting the operations and business objectives of our strategic business partners. To put this in context, approximately 98% of the 8.7 million e-filed tax returns that FTB expects to receive in 2006 will come to FTB through business stakeholders.

PIT e-file: FTB projects that 60% of the 14.7 million California PIT returns it receives in 2006 will be e-filed. Today, the majority of returns are e-filed using modems. By the end of 2007, the use of modems will be phased out, and FTB's e-file program will rely exclusively on FTB's Internet infrastructure for receiving e-file returns. By 2010, FTB estimates that nearly 70% of California PIT returns will be e-filed.

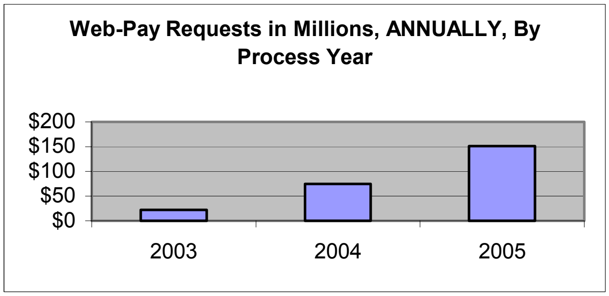


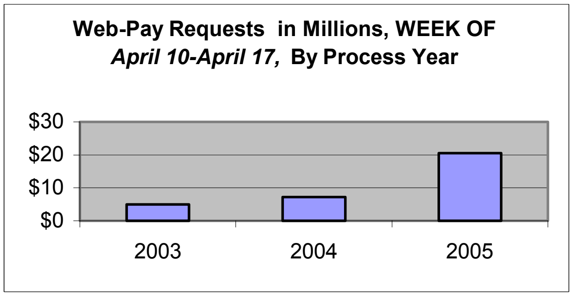
Business e-file: In 2006, FTB expanded its electronic tax return filing program by implementing the Business e-file program. By 2010, FTB expects that more than 25% of the one million California business returns filed each year will be e-filed. Business e-file relies exclusively on the Internet to receive these returns.[2]



[2] FTB Filing Division Town Hall Presentation, October 5, 2005.

Additional e-commerce applications: FTB employs 26 additional e-commerce programs that perform important revenue-collection, processing, and customer service functions, with three new programs slated to go online in the next year.[3] Two key e-commerce applications are INC (Integrated Non-Filer Compliance) and Web Pay. INC allows taxpayer to respond to notices issued for failure to comply with California's filing requirements. Web Pay allows taxpayers to request electronic payment of their state tax obligations.





Internet Infrastructure: FTB's current Internet infrastructure was originally designed to support only FTB's static Website. As FTB's business areas raced to respond to the public's and state policy demands for electronic services, the department was forced to react by quickly adding e-commerce applications to an Internet infrastructure that was not designed or funded to support them.

A "single point of failure" is like a weak link in a chain. If that weak link breaks, the entire chain is broken. A "fault-tolerant" Internet infrastructure has no weak links because it is made up of dual, or "redundant," devices capable of performing the same functions. When one device fails or is down for service, its "redundant" twin takes over to perform that function. In this way, the Internet infrastructure remains unbroken, allowing e-commerce programs to remain available.

FTB's Internet infrastructure was built in a piecemeal fashion, quickly, inexpensively and with minimal overall regard to a master plan, and, as such, has multiple single points of failure. Lack of a master-planned, "scalable" Internet infrastructure makes adding new e-commerce projects complex, time-consuming and expensive. In addition, FTB's Internet infrastructure was not designed to contend with today's more hostile security environment.

3.2 Business Problem/Opportunity

1. **The existing Internet infrastructure contains multiple single points of failure that jeopardize FTB's ability to provide virtually uninterruptible e-commerce availability to its internal and external customers.**

   Risk of e-commerce unavailability due to planned downtime: Because so many of the devices that make up FTB's Internet infrastructure are "single points of failure," taking one of these

[3] **HOH Application** will allow electronic submission of Head of Household questionnaire; **Web Demand** will permit the submission of electronic requests to release liens; **On-line 1099 Filing** will allow 1099 recipients to view their 1099s using FTB's website.

devices down for service is problematic because it also takes down the entire Internet infrastructure. E-commerce may cease until the device being repaired is put back into service.

FTB tries to schedule infrastructure device maintenance during other scheduled maintenance windows, but this is not always possible. As the number and sophistication of security threats increases, Internet infrastructure devices must be serviced more often to apply the upgrades and "patches" needed to combat these threats.

FTB has an opportunity to come closer to the need for 24x7x365 Internet infrastructure availability by eliminating single points of failure in FTB's Internet infrastructure, allowing for both planned and unplanned/catastrophic Internet infrastructure downtime without impacting e-commerce availability.

Risk of e-commerce unavailability due to unplanned downtime/catastrophic failure: FTB's current Internet infrastructure design is not "fault tolerant" because it lacks redundant devices at several points, exposing FTB's Internet infrastructure to a relatively significant risk of future unplanned e-commerce downtime.

- Many of the devices that make up FTB's Internet infrastructure will soon be declared "end of life" by the vendor, which means within a few years the manufacturer will no longer support them.

- Many of the FTB Internet infrastructure's switches and routers are also single points of failure, which puts FTB's ability to provide virtually uninterruptible e-commerce availability at risk.

- A cut to the fiber-optic line connecting FTB's Butterfield Way campus to its ISP would cause FTB's Internet infrastructure and e-commerce programs to stop working.

In addition, some risk to FTB's Internet infrastructure is posed by the lack of dual Internet Service Providers (ISP) and redundant, separate physical locations:

- If FTB's Internet Service Provider experiences an outage, FTB's e-commerce availability would be impacted for the duration of that outage.

- Flooding due to a levee-break or 100-year flood level rainfall also could cause FTB's Internet infrastructure and e-commerce programs to stop working.

- FTB has been the object of bomb and other threats for decades. However, since the Oklahoma City bombing of the Federal Building in 1995 and the World Trade Center attacks on Sept. 11, 2001, FTB's concerns about physical security have grown. Having separate and "redundant" physical locations lays the foundation for a more secure, fault-tolerant e-commerce infrastructure

A catastrophic/unplanned Internet infrastructure failure would impact FTB's operations anytime but would cause more serious problems if it occurred in April (the peak PIT tax-filing month), or in October (FTB's busy period for business returns):

- FTB's e-commerce applications, including all of its e-file programs, would stop functioning.

- CalFile, one of FTB's most high-visibility e-commerce programs, would stop working on the busiest filing day of the year. CalFile is an FTB-designed, free PIT e-file program. If it crashed on April 15, the political consequences would be serious. Many would conclude that FTB's e-commerce offerings are unreliable and don't work. Thousands of taxpayers could decide to return to traditional paper filing methods.

- FTB has mandated that tax practitioners who use tax preparation software and file more than 100 PIT returns a year *must* e-file. An e-commerce outage would deny FTB's obligation to make e-file available to the same group of tax practitioners who have been *mandated* to use it.

- FTB's Call Centers – the Taxpayer Services Line, Tax Practitioner Hotline, e-file Help Desk, and Collections Call Center – would be impacted. Customer service would suffer as these call centers struggled to answer more calls than they are staffed to answer within a reasonable time.

- By far the biggest impact would be an overall loss of public confidence in the accuracy, reliability and security of all of FTB's e-commerce programs – and quite possibly in other state agency e-commerce programs - at a time when state policy and the State's Chief Information officer are urging the public to do business electronically with all state agencies, including FTB.

2. **FTB's current Internet infrastructure is exposed to a more hostile Internet environment, but it lacks some of the Event Correlation needed to ensure the continued privacy and confidentiality of customer information.**

    - **Security threat diagnosis and response times.** FTB's current Intrusion Detection system must manually diagnose network anomalies and is therefore slow to diagnose and respond to security threats. As a result, a security response could come too late to block a threat to FTB's confidential taxpayer information. FTB has an opportunity to acquire new consolidated event correlation tools that provide the analytical capabilities and automated alerts that enable FTB staff to quickly and successfully detect and combat security threats.

    - **Capacity to handle network traffic.** Network traffic sometimes exceeds the current Intrusion Detection infrastructure's capacity. At these times, malicious system attacks have the potential to go undetected, security threats could go unchallenged, and the security of confidential data may be at risk. FTB has an opportunity to install new Intrusion Prevention System modules with the ability to detect malicious traffic and block unwanted code, ensuring the security of FTB's confidential data.

    - **Ability to combat "Zero-day" and Denial of Service attacks.** These attacks send huge amounts of malicious electronic traffic to one or more of the devices that make up FTB's Internet infrastructure. This malicious traffic consumes so many system resources that the Internet infrastructure may be unable to support FTB's e-commerce applications. FTB has an opportunity to acquire new technology that will block malicious traffic in real time without affecting the flow of legitimate, mission-critical e-commerce transactions.

3. **FTB's current Internet infrastructure is not scalable and will be challenged to meet customers' increased demand for access to e-commerce services.**

   FTB's Internet infrastructure is handling a growing load of e-commerce applications and other electronic services. However, it was not master planned or funded to support its current or future e-commerce applications. As a result:

   - **Single points of failure** continue to be built into the infrastructure, and redundancy and fault tolerance are not addressed from an enterprise-wide point of view.

   - The **current Internet infrastructure is not "scalable,"** requiring a significant amount of additional time and money for infrastructure redesign when a new e-commerce application is added. New applications are added every year to meet the needs of taxpayers and of FTB's business partners.

   - **Continual redesign adds more complexity and change to the infrastructure**, which makes diagnosing and fixing Internet infrastructure problems more difficult and time consuming.

   FTB has an opportunity to incorporate new Internet infrastructure technology and design concepts and build a scalable Internet infrastructure. Doing so will make adding new e-commerce projects faster and less expensive, without impacting FTB's ability to diagnose and effectively respond to Internet infrastructure issues.

3.3 Business Objectives

The EPI project will address business problems/opportunities identified in the previous section of this report by achieving the following:

1. Provide a fault tolerant Internet infrastructure by project completion (11/2/09) that will bring FTB closer to the business need of 24x7x365 infrastructure availability by eliminating single points of failure from a network perspective, with the exception of dual physical locations and Internet Service Providers. (Business Problem/Opportunity #1)

2. Support e-commerce applications and activities with additional enhanced security capabilities by project completion (11/2/09) that preserve the continued privacy and confidentiality of FTB customers' information to comply with Internal Revenue Service (IRS) Publication 1075 ("Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information"). (Business Problem/Opportunity #2)

3. Provide a scalable infrastructure and design by project completion (11/2/09) to support e-commerce applications and activities, allowing e-commerce application components to be added to the Internet infrastructure with no significant infrastructure re-design required, and without adding single points of failure to the infrastructure. (Business Problem/Opportunity #3).

3.4 Business Functional Requirements

The following functional requirements support the business objectives articulated above:

The EPI project will provide a fault-tolerant Internet infrastructure design that will bring FTB closer to the business requirement of 24x7x365 infrastructure availability. (Business Objective 1)

1. Fault-tolerant network with 24x7x365 availability.
2. Firewalls with stateful failover and load balancing capability.
3. Redundant network routers, switches and firewalls
4. Dual network paths for applications.

The EPI project will support E-Commerce applications and activities with additional enhanced security components that preserve the continued privacy and confidentiality of FTB customers' information. (Business Objective 2)

5. Design that supports dual-authored firewall architecture.
6. Intranet secured zone protected by firewalls.
7. Intrusion Prevention Systems (IPS) that provide security surveillance for all zones of the EPI architecture.
8. IPS that provides denial of access and hacking protection.
9. Data integrity through real-time monitoring, detection, and blocking.
10. Secure management of all Internet infrastructure devices with automatic logging and reporting.

The EPI project will provide a scalable infrastructure to support e-commerce applications and activities. The Internet infrastructure will easily accommodate the continual implementation of e-commerce services and the rapid increase in demand for access to these services because infrastructure components can be virtualized without redesign. (Business Objective 3)

11. A resilient, scalable system that accommodates network traffic growth as the number of users increases.
12. Modular-based expandability through virtualization while minimizing equipment obsolescence.
13. Augmentation of the Internet infrastructure without significant redesign.
14. Component replacements (or expansion) that improves the system's reliability, availability and performance.
15. A system that supports emerging e-commerce applications.

4.0 Baseline Analysis

4.1 Existing Environment

Currently, FTB has one Internet Service Provider (ISP). This ISP is utilized for in-bound traffic by FTB's external customers and for outbound traffic by FTB employees in the transaction of business related activities. Employees also communicate with one another, with other State of California Agencies and other entities, such as the IRS.

A clustered firewall set protects the E-commerce DMZ, and intrusion detection sensors provide security for those engaged in business transactions, interactions and other services. Customers and employees utilize a variety of business applications and services that have been implemented because of approved initiatives and are supported by the E-Commerce departmental network infrastructure.

4.2 Technical Environment

The current Internet infrastructure supports an interface with multiple firewalls protecting its FTB E-Commerce and internal enterprise network. The Internet Network is secured by border routers with two PIX firewalls protecting two secure DMZ's. Nokia Checkpoint firewalls and one ISS RealSecure Intrusion Detection Sensors protect FTB's internal network.

The PIX firewalls are high-performance stateful packet-filtering firewalls. One pair of PIX firewall provides a gateway into the protected DMZ that houses the FTB Web servers, and the other pair of PIX firewall protects an E-Commerce zone where all the external web applications reside. A Cisco PIX firewall and a Cisco Local Director are configured in a standard E-Commerce DMZ configuration.

The Nokia Checkpoint firewall is an appliance based stateful firewall. There are two sets of Nokia Checkpoint firewalls that provide an extra layer of protection for the DMZ in FTB's internal network. One set of Nokia Checkpoint firewalls acts as gateway firewall for the internal FTB users to access the Internet, and provides connection to the E-commerce DMZ by protecting the internal FTB network from external users. A second set of Nokia Checkpoint firewalls protects the web development servers.

The ISS RealSecure Intrusion Detection Response System (IDRS) provides an extra layer of security in FTB's Internet architecture. The IDRS acts as an alarm that reports potential attacks or misuse at FTB's perimeter.

The existing Internet access point is provided through Electric Light Wave, Inc. (ELI) and consists of a point-to-point high speed OC-3 Circuit. The OC-3 circuit is set at a guaranteed minimum 20Mbps rate, capable of bursting up to the line rate of 155Mbps. The circuit terminates onto a Cisco 7500 router.

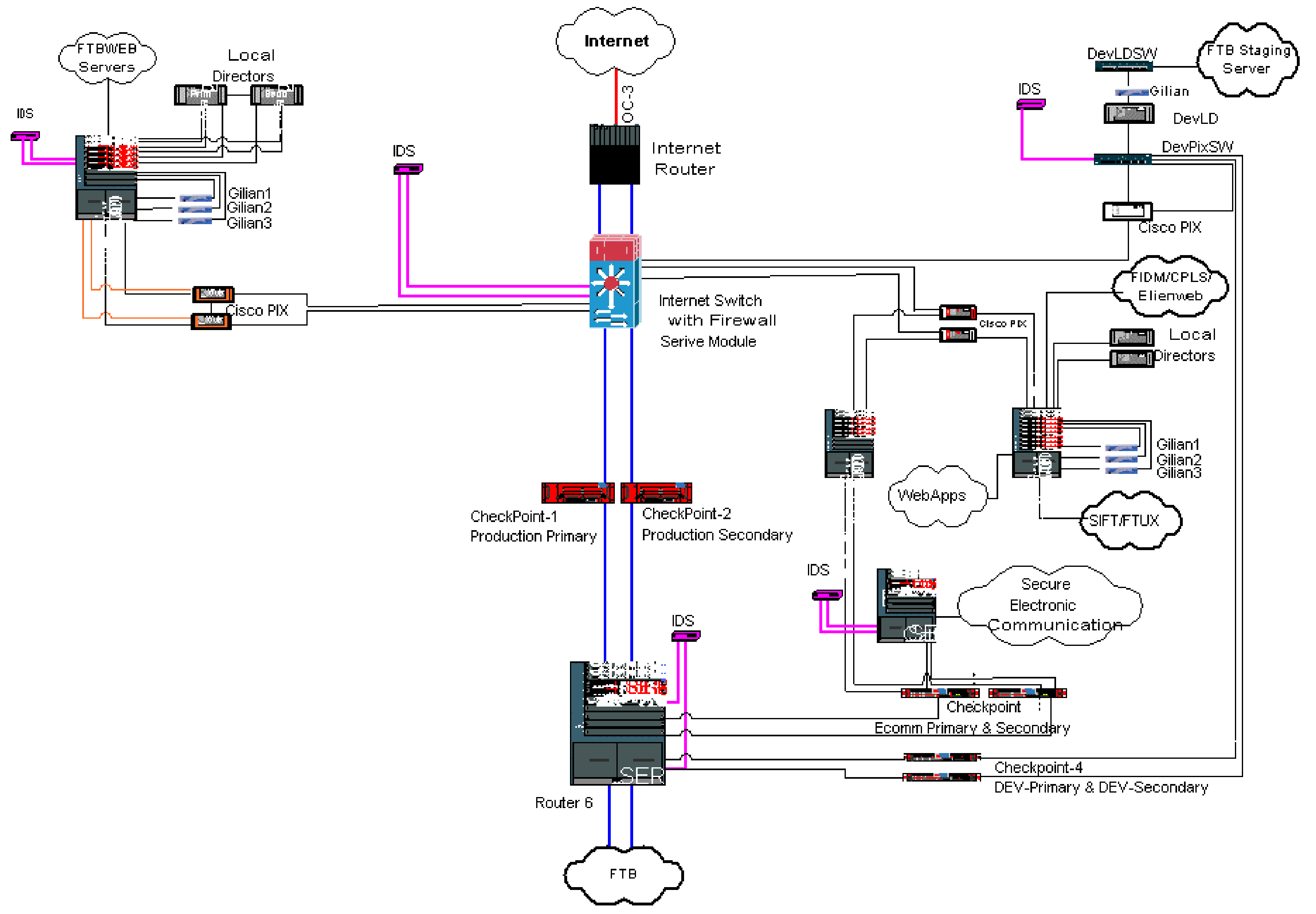
The Local Area Network (LAN) at FTB's campus is the heart of the enterprise network, providing reliability and scalability throughout FTB. There are approximately 6,000 clients supported on the network. Network users have access to the various system applications via infrastructure devices such as routers, switches, hubs and the mainframe Open Standard Adapters. The current enterprise network topology incorporates over 100 Gigabit Ethernet data switches that primarily use the TCP/IP protocol suite.

The campus topology follows a three-tier enterprise model. This model consists of three distinct functional layers: core, distribution and access. The core layer is a Ten Gigabit Ethernet switched backbone network, which redundantly interconnects the distribution layer switches in the Sacramento, San Francisco, Los Angeles and San Diego Buildings.

The distribution layer switches connect to over seventy access layer switches, which terminate to workstations and other network end devices. Additionally, there are a total of three server farm switch environments located in three of the four buildings. These server farm switch environments provide fault tolerance to the enterprise servers.

The Metropolitan Area Network is comprised of the International Drive and Micron suites. They access FTB's campus via Asynchronous Transfer Mode (ATM) over Synchronous Optical Network (SONET) at OC-3 speed with a switched Fast-Ethernet LAN technology. The Wide Area Network incorporates redundant and encrypted frame relay communication links to the In and Out of State field offices. The remote environments incorporate a mixture of over 40 data switched Ethernet hubs for their local network communications.

Existing Internet Infrastructure Schema



Franchise Tax Board-DMZ
Network Management Bureau

5.0 Proposed Solution (See also Diagram 1, Page 14)

Internet Public Access Zone

Within the Internet Public Access Zone is one Internet Service Provider (ISP) utilizing OC3 connectivity. This circuit will provide a maximum bandwidth of 155 megabits per second. The ISP will be connected to two [redacted] series routers (Edge Router). Backup connectivity between the ISP to the routers will be provided by "dark" (inactive) fiber that can be activated in case the primary fiber connection is cut. An Intrusion Prevention Sensor (IPS) and Distributed Denial of Service Detector (DDOS) will protect this zone. In addition, access control lists (ACL) at the Edge Router will limit exposure by allowing communication to specific ports into the Extranet Secured Zone.

Extranet Secured Zone

The purpose of the Extranet Secured Zone is to provide a buffer that has no direct linkage between the Internet and FTB's Intranet Secured Zone. This zone provides access control, protocol filtering, authentication, intrusion prevention and DDOS prevention.

The proposed Extranet Secured Zone consists of redundant Checkpoint and Cisco Firewalls. These firewalls will provide a first and second layer of defense, respectively. The Checkpoint Firewalls will provide load-balancing using cluster technology. The Cisco Firewall Service Modules (FWSM) are integrated into the Edge Distribution Switch Block. These FWSMs are scalable to virtual Firewalls (Contexts) that can be utilized for current and future E-Commerce applications. Both Checkpoint and Cisco Firewalls will offer high performance, deep packet inspection and fault-tolerance.

The Application Control Engine (ACE) modules are integrated into the Extranet Server Farm Switch Block. These modules will provide server load-balancing and Secure Socket Layer (SSL) offloading. Just like the FWSM, the ACE module can also be virtualized and associated to FWSM contexts.

The virtualized contexts host a multitude of business applications, such as WEB, Transaction, Multimedia, Proxy Services, Employee Services, Partner/Vendor Services, Application Staging Services, Application Development Services, etc.

Intranet Secured Zone

The Intranet Secured Zone provides an additional layer of security and data integrity for internal server farms that provide public services.

The FWSM and ACE modules are integrated within the E-Commerce Back-End Switch Block These modules will provide security, server load-balancing and Secure Socket Layer (SSL) offloading. The virtualized contexts host a multitude of internal business applications, such as Application Staging, Application Development, Database Services, etc.

Network Analysis Modules (NAM):

NAMs are integrated into the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block. This NAM is a tool for Network Analysts that will identify application flows, protocol distribution, perform trend analysis, and capacity management. All collected data from these NAMs will be used to optimize application behavior, anomaly detection and isolate network problems.

Application Velocity System (AVS):

AVS appliances are connected to the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block. This AVS appliance has a built-in application security firewall, which will identify and prevent application layer threats and data theft. These appliances provide acceleration, monitoring and securing web-based application delivery to all connected clients with out modifying clients or servers. The AVS appliance manages all client sessions by consolidating similar data sessions into a single session destined for the application server. So, all E-Commerce applications over HTTP or HTTPS are optimized with greater response time and reduced bandwidth requirements.

Intrusion Detection/Prevention System (ID/PS):

The Intrusion Detection/Prevention System consists of VPN/Security Management Solution (VMS); network intrusion detection sensors (NIDS); Host Intrusion Detection Sensors (HIDS); and [redacted]

VMS will provide security management capabilities to help meet the overall security needs. VMS also allows security analysts to manage and troubleshoot the configuration and the policies of NIDSs, HIDs, and firewalls.

The NIDS modules are integrated into the Internet Edge Distribution Switch Block, and the E-Commerce Back-End Switch Block. These NIDS modules will provide promiscuous inspection of network traffic, which will send an alert based on a signature-driven event. These events are also sent to the [redacted] for event correlation and validation.

The HIDS safeguards the entire server by preventing known and unknown malicious attacks such as Web defacement, buffer overflows, worms, newly discovered attacks, zero-day, etc. By blocking these attacks, the HIDS significantly decreases downtime and protects critical assets. The HIDS uses a combination of behavioral rules and signatures to prevent known and unknown attacks.

The [redacted][4] is an appliance-based solution that provides insight and control of the existing security deployment. The [redacted] allows the FTB to identify, manage, and counter security threats. It works with our existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution.

[redacted] transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. This threat mitigation appliance enables security analysts to centralize, detect, mitigate, and report on priority threats using the network and security devices

[4] The [redacted] has been identified for costing purposes only since no product at this time can meet the proposed configurations. However, other products, including the current solution in place (ISS), will be evaluated to determine the most effective solution for FTB.

already deployed within the EPI. This product supports log data from various security Hardware/Software solutions such as, vulnerability assessment tools, Antivirus, Windows 2000, and 2003 logs, etc.

Summary

The new architecture and design presented in this solution will provide a high level of security with "zero-day" threat mitigation, fault-tolerance, dual network paths and scalability for future growth.

Securing Franchise Tax Board's resources is the top priority of the EPI Project. The design details are sound and are composed of a complex labyrinth of security controls whose span extends from the Internet Public Access Zone to the Intranet Secured Zone. These controls are made up of dual-authored firewalls; an Intrusion Detection and Prevention System; Distributed Denial of Service Prevention System; and an Event Correlation System. This creates a highly secured transaction environment that is self-defending and that will protect the customer.

E-commerce infrastructure reliability is key to supporting a 24/7/365 uptime. The EPI Project, by design, accomplishes this by incorporating network redundancy across components and devices. This methodology of redundancy promotes a self-healing environment that can prevent the loss revenue.

As FTB's participation in e-commerce grows and business requirements constantly change, the network infrastructure must have the ability to keep up. The EPI Project addresses this need by using a concept called "virtualization." Virtualization is the ability to create multiple environments on one infrastructure device or a group of devices. These environments allow a single device or group of devices to accommodate new e-commerce programs, so there's no need to purchase new equipment.

Many of the network devices used in this project support this concept and as a result, environments can be added or removed seamlessly. For example, the Extranet and Intranet Secured Zones host a set of secure environments. As new applications are created, new environments to accommodate these applications can be set up in a timely and cost effective manner.

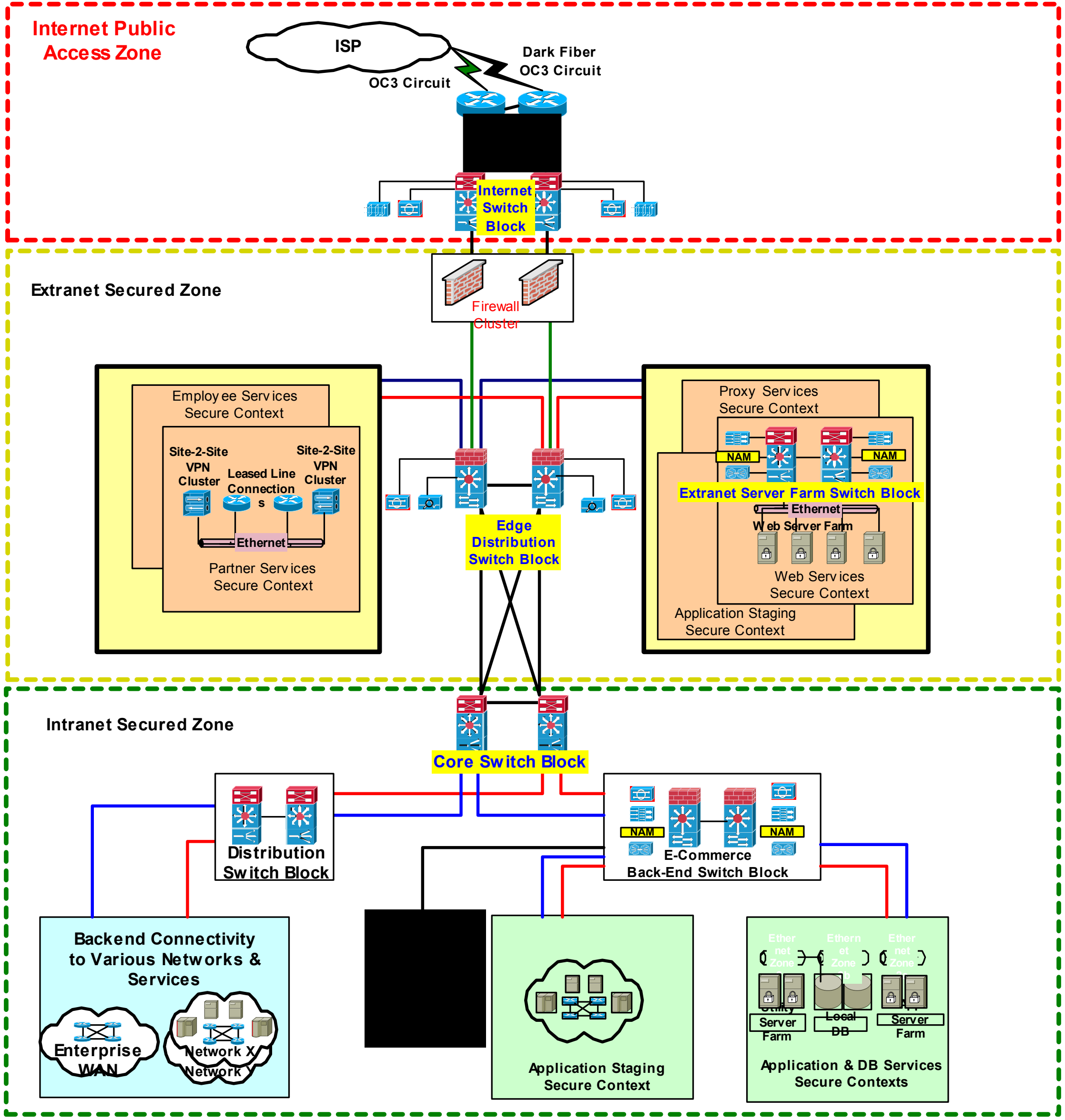
Advantages:

1. Same physical location: easier to manage
2. Load balancing and redundancy at the infrastructure level
3. Session based fault tolerance
4. Simplified security (Taxpayer data kept on site)
5. Easier contracts
6. No IAA needed
7. Less equipment and one Internet Service Provider means lower cost

Disadvantages:

1. Lacks redundant Internet Service Providers; ISP outage will interrupt e-commerce.
2. Lacks site redundancy; site outage will interrupt e-commerce.

FTB E-Commerce Portal Infrastructure (EPI) Proposed Solution, Diagram 1


Internet Public Access Zone
ISP
OC3 Circuit
Dark Fiber OC3 Circuit
Internet Switch Block
Extranet Secured Zone
Firewall Cluster
Employee Services Secure Context
Site-2-Site VPN Cluster
Leased Line Connection
s
Site-2-Site VPN Cluster
Ethernet
Partner Services Secure Context
Edge Distribution Switch Block
Proxy Services Secure Context
NAM
NAM
Extranet Server Farm Switch Block
Ethernet
Web Server Farm
Web Services Secure Context
Application Staging Secure Context
Intranet Secured Zone
Core Switch Block
Distribution Switch Block
NAM
NAM
E-Commerce Back-End Switch Block
Backend Connectivity to Various Networks & Services
Enterprise WAN
Network X Network
Application Staging Secure Context
Ethernet Zone
Ethernet Zone 2b
Ethernet Zone
Utility Server Farm
Local DB
Server Farm
Application & DB Services Secure Contexts

[redacted]

[redacted]

Revision 10 Date 11/07/2006

Legend

- Server w/ Host based IPS
- Application Velocity Pipeline/Security Services
- IDS/IPS Services
- DDOS Guard
- DDoS Detector
- Content Load Balancing Services with SSL offloading
- Multi-layer Switch w/Integrated FW and Multiple Secure Contexts
- Multi-layer Switch
- Global Site Selector

[redacted]

5.1 Solution Description

1. Hardware:

Item	Amount
Nokia CheckPoint Firewalls	237,990
Nokia CheckPoint Maintenance	36,000
Cisco Routers, Switches, Firewalls, ACE, NAM, AVS	1,368,749
Cisco Equipment Maintenance	156,829
[redacted]	612,790
[redacted]	48,874
Sub Total	2,461,412
Tax	190,759
Total Hardware	**$ 2,652,171 ***

2. Software:

Item	Amount
CheckPoint Licenses	9,860
Cisco Host IDS Software (IDRT Security)	150,577
Cisco Software Maintenance (IDRT Security)	34,446
Sub Total	194,883
Tax	15,103
Total Software	**$ 209,986 ***

Internet Service Provider (ISP)	
ISP ELI Service cost per Year	57,300
Cabinets & Wiring	116,280
Sub-Total	173,580
Tax	13,452
Total Tele-Communication	**$ 187,032 ***

* Costs reflected differently in the EAWs. These costs do not include interest charges as part of the 3-Year Financing Option.

3. **Technical platform:** The EPI Project if approved would be the platform.

4. **Development approach:** FTB staff, with the assistance of a contractor, will design, install, configure, establish all technical interfaces, test and migrate all infrastructure devices.

5. **Integration issues:** FTB will be migrating from the existing infrastructure configuration to the EPI Infrastructure. FTB will be converting its external IP addressing scheme to a different IP scheme. The Domain Name Server table will need to be updated. Related application devices will be migrated at the same or different times based on the dependency of those

devices. All internal e-commerce application and database servers will be migrated to the Internal Secure Zone.

6. **Procurement approach:** This project will require three procurements. Each of these procurements will be completed through competitive bidding processes such as CMAS (Request for Offer process), MSA, or through a Request for Quote (RFQ).

   - Project Oversight and Validation
   - Hardware and Software
   - Technical Consultant(s)

   An Information Technology Procurement Plan (ITPP) will be prepared and submitted to the Department of General Services for review and approval prior to conducting any procurements associated with this project. The ITPP will describe the overall strategy necessary to accomplish and manage the acquisitions required for this project by formally documenting that the proposed approach for the acquisition satisfies state requirements. The ITPP will serve as a reference document and become a permanent record of acquisition decisions. See Project Schedule (section 6.5.5) for Key Procurement Milestones/Tasks.

7. **Technical interfaces:**
   - Internet
   - Web servers
   - Application servers
   - Transaction servers
   - Development servers
   - Database servers
   - E-commerce application servers
   - Secured Electronic Communication servers
   - SWIFT appliances
   - Centralized Authentication Project (CAP) servers.

8. Testing of all network equipment will begin upon arrival of the equipment. The equipment will be installed into racks, and burn-in testing will be performed. Network staff, working with the consultant, will interconnect all equipment with cables, perform configurations, and test for basic system connectivity. Network staff and the consultant will apply security policies, and Security staff will then perform security scans to test for system vulnerability. Network and Security staff, working with the consultant, will implement the Intrusion Prevention System (IPS) by collecting all the logs into the [redacted] system. Once Security staff certifies the security of the EPI system, Network staff will work with the consultant and with FTB's various e-commerce application groups to migrate FTB's e-commerce applications from the existing infrastructure to the new e-commerce portal infrastructure.

9. **Resource requirements:** 18.5 PYs required for one-time activities and 11.2 PYs of staff required for on going support, due to increased complexity and the increased workload in monitoring activities.

- 2.0 PYs are required for the installation, configuration, and on-going maintenance to support the increased capacity of the new E-Commerce network Intrusion Detection System (IDS) infrastructure. The new infrastructure will be scalable to accommodate future E-Commerce application requirements, and will require 24 by 7 monitoring and availability. These 2 additional PYs will need to inspect the entire traffic stream traversing to and from the Internet (unsecured zone) and Intranet (secure zone) across a 10-gigabit (GB) network backbone with multiple network segments.

- PY Needs by Fiscal Year
    - FY 2006/07
        - One-Time: 0.8 PYs
        - Continuing IT (On-going): 0.0 PY
    - FY 2007/08
        - One-Time: 5.5 PYs
        - Continuing IT (On-going): 0.0 PY
    - FY 2008/09
        - One-Time: 9.0 PYs
        - Continuing IT (On-going): 0.0 PYs
    - FY 2009/10
        - One-Time: 3.2 PYs
        - Continuing IT (On-going): 7.5 PYs
    - FY 2010/11
        - One-Time: 0.0 PYs
        - Continuing IT (On-going): 11.2 PYs
    - TOTALS:
        - One-Time: 18.5 PYs
        - Continuing IT (On-going): 11.2 PYs

10. **Training plan:** The FTB network operations and security staff will require formal classroom training for Internet infrastructure, device, and security component administration. They will be responsible for configuring, installing and maintaining/supporting/troubleshooting individual devices and components and the overall Internet infrastructure. Contractor staff will be responsible for knowledge transfer to state staff.

11. **Ongoing maintenance:** After implementation, 11.2 PYs will provide ongoing Internet infrastructure maintenance.

12. **Information security:** Security features to protect confidentiality of data and information are an integral part of this Alternative. This proposed solution will meet FTB's security requirements as described in the Department's Information Security Manual and in Internal Revenue Service (IRS) Publication 1075 (”Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information”).

13. **Confidentiality:** Because of the fault tolerant nature of the solution, FTB's services will be available 24x7x365. The integrity, confidentiality and privacy of information will be ensured because of the many security enhancements.

14. **Impact on end users:** The impact on end users will be transparent.

15. **Impact on existing system:** This project will replace the existing infrastructure with a new design. The new infrastructure will add a fault-tolerant network to expand and grow FTB's e-commerce capability.

16. **Consistency with overall strategies:** The E-Commerce Portal Infrastructure project supports the following strategic goals of the Franchise Tax Board:
    - Goal 1, Become Customer-Centered, by making it easier for customers to access and use products and services, empower taxpayers and others to resolve their issues through convenient self-service options.
    - Goal 2, Promote Fair & Effective Tax Administration, by supporting e-commerce applications that increase the percentage of returns that are filed on time and error-free, helping to identify non-filers, and making filing returns as easy and fair as possible.
    - Goal 4, Deliver Efficient and High-Quality Business Results, which capitalize on opportunities to improve efficiency through implementation of electronic processes and services, and
    - Goal 5, Protect Taxpayer Privacy and Ensure Security of Taxpayer information by implementing an Internet infrastructure, including enhanced Internet infrastructure security components, that is consistent with the Department's architectural standards for confidentiality of taxpayer information, using industry best practices for information security.

17. **Impact on current infrastructure:** (See #15 above)

18. **Impact on data center(s):** None.

19. **Data center consolidation:** FTB is a "single-agency, dedicated use data processing center". Data Center consolidation does not apply to FTB

20. **Back-up and operational recovery plan (ORP)**: The proposed E-Commerce Portal Infrastructure project will replace FTB's existing Internet infrastructure, which supports all of FTB's e-commerce systems. FTB's Business Impact Assessment defines the FTB Internet infrastructure as a Tier 0 recovery priority with a Recovery Time Objective of less than 24 hours. FTB's goal for the Internet infrastructure is zero downtime.

    Business resumption plans are in place for FTB's Internet infrastructure. The Network Management Bureau will maintain the proposed system once implemented. The existing NMB resumption plans will be revised to reflect the new Internet infrastructure's redundancy and fault tolerance. One of the benefits of the EPI project is disaster mitigation. This project will make FTB Internet infrastructure more fail-safe, minimize recovery actions and minimize the need to implement FTB disaster recovery plan. This will also be reflected in the Operational Recovery Plan (ORP) submitted to the Department of Finance annually.

21. **Public access:** The proposed solution does not provide direct public access to State database by private sector organizations or individuals.

22. **Costs and benefits:** See Section 8.0, EAWs, for cost detail.

One-time cost: $5,909,435 for hardware, software, contract services and 18.5 PYs.

- Hardware - $2,833,359 (with financing over 3 years)
- Software - $224,331 (with financing over 3 years)
- Telecommunications - $199,809 (with financing over 3 years)
- Contract Services (Design Consulting) - $357,888 (with financing over 3 years)
- IV&V Services - $242,279
- DGS Analyst - $20,150
- Personnel Services - $1,799,259
- Training - $232,359 (with financing over 3 years)

On-going Maintenance and Operations Cost: $1,437,766 for hardware/software maintenance and 11.2 PYs.

- Hardware Maintenance - $216,242
- Software Maintenance - $45,585
- Telecommunications - $123,195
- Personnel Services - $1,052,744

This project will provide a new Internet infrastructure that will enable FTB to better satisfy customers' demand by delivering quality e-commerce services in a secured and fault tolerant environment. These are non-financial benefits and cannot be easily quantified and measured.

23. **Sources of funding:** Redirection and Budget Change Proposals (BCPs). The FSR proposes to obtain project funding through a BCP for FY 07/08, FY 08/09, FY 09/10 and FY 10/11.

5.2 Rationale for Selection

The EPI Proposed Solution is based on security, and redundant and scalable configurations. It does not address redundant ISPs and two separate locations because the risks to FTB's Internet infrastructure by these factors are relatively low. However, the costs associated with mitigating these risks are quite high. At a time of constrained budgets, FTB is proposing a cost-effective solution that effectively addresses the highest-risk issues facing its Internet infrastructure and e-commerce availability.

If FTB does not implement the Proposed Solution, some of the infrastructure to support planned e-commerce initiatives is likely to be implemented in a piecemeal fashion. However, it is because of adding to the infrastructure in a segmented, piecemeal, "stovepipe" approach that it is now difficult to manage and diagnose problems within the infrastructure.

The infrastructure has simply evolved over time by accommodating new business applications with the addition of more components. Also, the current infrastructure has very limited fault tolerance. In addition, the current network infrastructure does not have the optimal level of required security or scalability for future growth. All of these factors present a significant risk for the FTB to carry out its mission of collecting revenue and administering the California Revenue and Taxation Code.

The EPI Project will provide FTB with a robust e-commerce Internet infrastructure that will assist in ensuring successful revenue collection now and in the future. Recognizing the value and the necessity of a secure, stable, scalable, self-defending and self-healing network infrastructure are the strategic concepts that have guided the planning and design of the EPI project.

5.3 Describing Alternatives:

5.3.1 Alternative 1 (See also Diagram 2, Page 24)

In design Alternative 1, the Internet infrastructure would be located entirely on the FTB campus but would include two rather than one Internet Service Provider for redundancy. Alternative 1 would provide FTB with a high level of security, fault-tolerance, and scalability. The infrastructure is comprised of three zones, Internet Public Access Zone, Extranet Secured Zone, and an Intranet Secured Zone.

Internet Public Access Zone

Within the Internet Public Access Zone are two ISPs utilizing OC3 connectivity. These circuits will provide us a maximum bandwidth of 155 megabits per second. Each ISP will be connected to [redacted] series routers (Edge Router) using the Border Gateway Protocol (BGP). Traffic will be distributed via DNS load balancing using Cisco's Global Site Selector (GSS). An Intrusion Prevention Sensor (IPS) and Distributed Denial of Service Detector (DDOS) will protect this zone. In addition, access control lists (ACL) at the Edge Router will limit exposure by allowing communication to specific ports into the Extranet Secured Zone.

Extranet Secured Zone

The purpose of the Extranet Secured Zone is to provide a buffer that has no direct linkage between the Internet and FTB's Intranet Secured Zone. This zone provides access control, protocol filtering, authentication, intrusion prevention and DDOS prevention.

The proposed Extranet Secured Zone consists of redundant Checkpoint and Cisco Firewalls. These firewalls will provide a first and second layer of defense, respectively. The Checkpoint Firewalls will provide load-balancing using cluster technology. The Cisco Firewall Service Modules (FWSM) are integrated into the Edge Distribution Switch Block. These FWSMs are scalable to virtual Firewalls (Contexts) that can be utilized for current and future E-Commerce applications. Both Checkpoint and Cisco Firewalls will offer high performance, deep packet inspection and fault-tolerance.

The Application Control Engine (ACE) modules are integrated into the Extranet Server Farm Switch Block. These modules will provide server load-balancing and Secure Socket Layer (SSL) offloading. Just like the FWSM, the ACE module can also be virtualized and associated to FWSM contexts.

The virtualized contexts host a multitude of business applications, such as WEB, Transaction, Multimedia, Proxy Services, Employee Services, Partner/Vendor Services, Application Staging Services, Application Development Services, etc.

Intranet Secured Zone

The Intranet Secured Zone provides an additional layer of security and data integrity for internal server farms that provide public services.

The FWSM and ACE modules are integrated within the E-Commerce Back-End Switch Block These modules will provide security, server load-balancing and Secure Socket Layer (SSL) offloading. The virtualized contexts host a multitude of internal business applications, such as Application Staging, Application Development, Database Services, etc.

Network Analysis Modules (NAM):

NAMs are integrated into the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block. This NAM is a tool for Network Analysts that will identify application flows, protocol distribution, perform trend analysis, and capacity management. All collected data from these NAMs will be used to optimize application behavior, anomaly detection and isolate network problems.

Application Velocity System (AVS):

AVS appliances are connected to the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block. This AVS appliance has a built-in application security firewall, which will identify and prevent application layer threats and data theft. These appliances provide acceleration, monitoring and securing web-based application delivery to all connected clients with out modifying clients or servers. The AVS appliance manages all client sessions by consolidating similar data sessions into a single session destined for the application server. So, all E-Commerce applications over HTTP or HTTPS are optimized with greater response time and reduced bandwidth requirements.

Intrusion Detection/Prevention System (ID/PS):

The Intrusion Detection/Prevention System consists of VPN/Security Management Solution (VMS); network intrusion detection sensors (NIDS); Host Intrusion Detection Sensors (HIDS); and [redacted]

VMS will provide security management capabilities to help meet the overall security needs. VMS also allows security analysts to manage and troubleshoot the configuration and the policies of NIDSs, HIDs, and firewalls.

The NIDS modules are integrated into the Internet Edge Distribution Switch Block, and the E-Commerce Back-End Switch Block. These NIDS modules will provide promiscuous inspection of network traffic, which will send an alert based on a signature-driven event. These events are also sent to the [redacted] for event correlation and validation.

The HIDS safeguards the entire server by preventing known and unknown malicious attacks such as Web defacement, buffer overflows, worms, newly discovered attacks, zero-day, etc. By blocking these attacks, the HIDS significantly decreases downtime and protects critical assets. The HIDS uses a combination of behavioral rules and signatures to prevent known and unknown attacks.

The [redacted][5] is an appliance-based solution that provides insight and control of the existing security deployment. The [redacted] allows the FTB to identify, manage, and counter security threats. It works with our existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution.

[redacted] transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. This threat mitigation appliance enables security analysts to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed within the EPI. This product supports log data from various security Hardware/Software solutions such as, vulnerability assessment tools, Antivirus, Windows 2000, and 2003 logs, etc.

Summary

The new architecture and design presented in this solution will provide a high level of security with “zero-day” threat mitigation, fault-tolerance, dual network paths and scalability for future growth.

Securing Franchise Tax Board’s resources is the top priority of the EPI Project. The design details are sound and are composed of a complex labyrinth of security controls whose span extends from the Internet Public Access Zone to the Intranet Secured Zone. These controls are made up of dual-authored firewalls; an Intrusion Detection and Prevention System; Distributed Denial of Service Prevention System; and an Event Correlation System. This creates a highly secured transaction environment that is self-defending and that will protect the customer.

E-commerce infrastructure reliability is key to supporting a 24/7/365 uptime. The EPI Project, by design, accomplishes this by incorporating network redundancy across components, and devices. This methodology of redundancy promotes a self-healing environment that can prevent the loss revenue.

As FTB’s participation in e-commerce grows and business requirements constantly change, the network infrastructure must have the ability to keep up. The EPI Project addresses this need by using a concept called “virtualization.” Virtualization is the ability to create multiple environments on one infrastructure device or a group of devices. These environments allow a single device or group of devices to accommodate new e-commerce programs, so there’s no need to purchase new equipment.

[5] The [redacted] has been identified for costing purposes only since no product at this time can meet the proposed configurations. However, other products, including the current solution in place (ISS), will be evaluated to determine the most effective solution for FTB.

Many of the network devices used in this project support this concept and as a result, environments can be added or removed seamlessly. For example, the Extranet and Intranet Secured Zones host a set of secure environments. As new applications are created, new environments to accommodate these applications can be set up in a timely and cost effective manner.

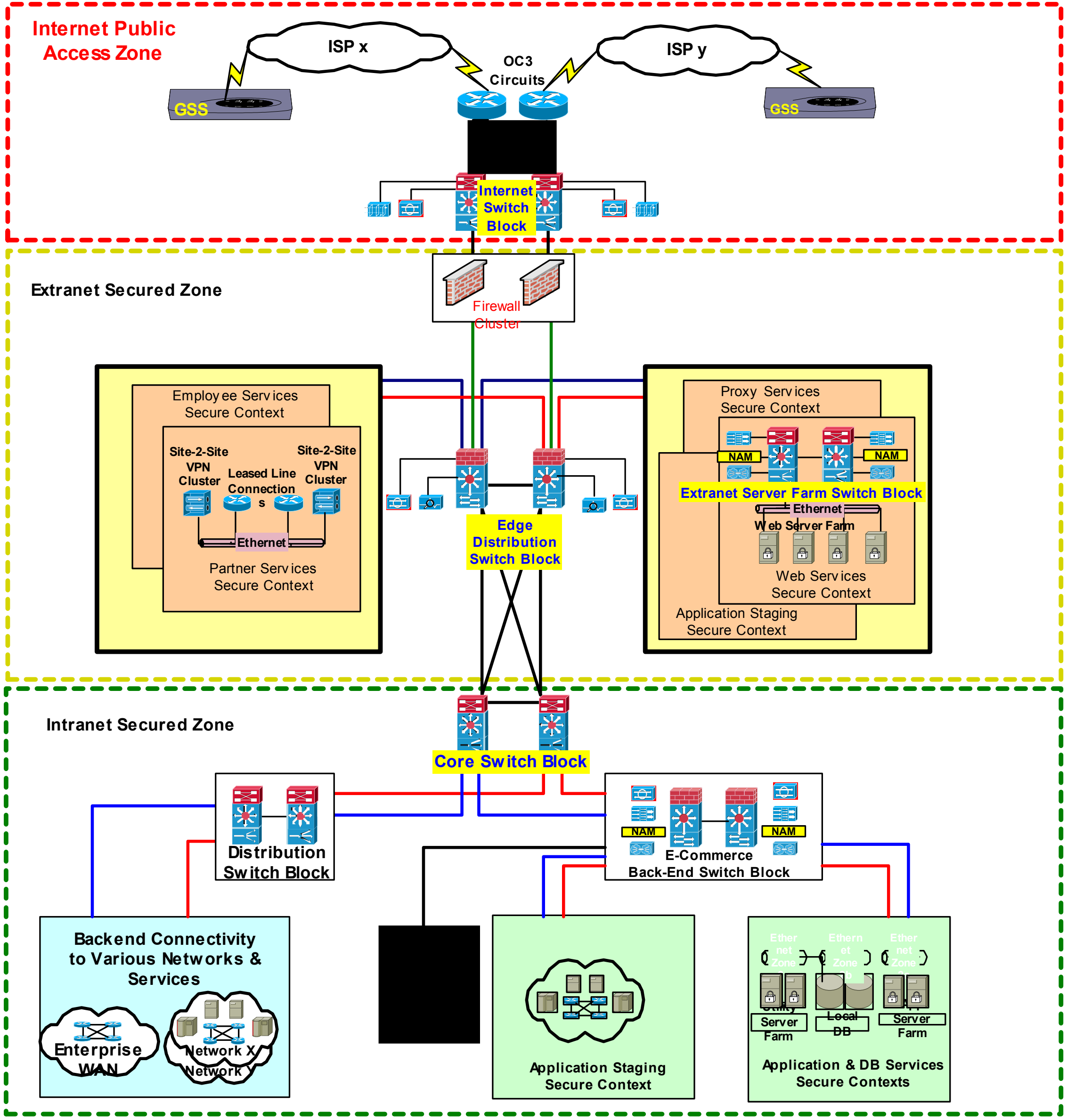
Advantages:

1. Same physical location: easier to manage
2. Load balancing and redundancy
3. Session based fault tolerance
4. Simplified security (Taxpayer data kept on site)
5. Easier contracts
6. No IAA needed
7. Less equipment, less cost

Disadvantages:

1. Lacks site redundancy; site outage will bring down the entire e-commerce presence.

FTB E-Commerce Portal Infrastructure (EPI) Diagram 2


Internet Public Access Zone
ISP x
ISP y
OC3 Circuits
GSS
GSS
[redacted]
Internet Switch Block
Extranet Secured Zone
Firewall Cluster
Employee Services Secure Context
Site-2-Site VPN Cluster
Leased Line Connections
Site-2-Site VPN Cluster
Ethernet
Partner Services Secure Context
Edge Distribution Switch Block
Proxy Services Secure Context
NAM
NAM
Extranet Server Farm Switch Block
Ethernet
Web Server Farm
Web Services Secure Context
Application Staging Secure Context
Intranet Secured Zone
Core Switch Block
Distribution Switch Block
NAM
NAM
E-Commerce Back-End Switch Block
Backend Connectivity to Various Networks & Services
Enterprise WAN
Network X Network
[redacted]
Application Staging Secure Context
Utility Server Farm
Local DB
Server Farm
Application & DB Services Secure Contexts

Revision 10 Date 11/07/2006

Legend

- Server w/ Host based IPS
- Application Velocity Pipeline/Security Services
- IDS/IPS Services
- DDOS Guard
- DDoS Detector
- Content Load Balancing Services with SSL offloading
- Multi-layer Switch w/Integrated FW and Multiple Secure Contexts
- Multi-layer Switch
- Global Site Selector

[redacted]

5.3.2 Alternative 2 (See also Diagram 3, Page 29)

As Diagram 3 shows, Alternative 2 would consist of two Internet infrastructures at two separate physical locations: one at Department of Technology Services, and the other at FTB's Butterfield Way campus. Each of the two Internet infrastructures features similar functionalities, and each has an independent circuit to its own ISP. Both infrastructure locations could actively support FTB's e-commerce traffic. This design could provide FTB with a high level of security, fault-tolerance, and scalability. Each location is comprised of three zones: an Internet Public Access Zone, an Extranet Secured Zone, and an Intranet Secured Zone.

Internet Public Access Zone

Within the Internet Public Access Zone are two ISPs utilizing OC3 connectivity. One ISP (ISPx) would be located at Franchise Tax Board (FTB) and the other ISP (ISPy) at the Department of Technology Services (DTS). Both ISPs would operate at the same time. These circuits would provide us a maximum bandwidth of 155 megabits per second. Each ISP would be connected to [redacted] series routers (Edge Router) using the Border Gateway Protocol (BGP). Traffic would be distributed between both sites via DNS load balancing using Cisco's Global Site Selector (GSS). An Intrusion Prevention Sensor (IPS) and Distributed Denial of Service Detector (DDOS) would protect this zone. In addition, access control lists (ACL) at the Edge Router would limit exposure by allowing communication to specific ports into the Extranet Secured Zone.

Extranet Secured Zone

The purpose of the Extranet Secured Zone is to provide a buffer that has no direct linkage between the Internet and FTB's Intranet Secured Zone. This zone provides access control, protocol filtering, authentication, intrusion prevention and DDOS prevention.

The proposed Extranet Secured Zone consists of redundant Checkpoint and Cisco Firewalls. These firewalls would provide a first and second layer of defense, respectively. The Checkpoint Firewalls would provide load-balancing using cluster technology. The Cisco Firewall Service Modules (FWSM) are integrated into the Edge Distribution Switch Block at each site. These FWSMs are scalable to virtual Firewalls (Contexts) that can be utilized for current and future E-Commerce applications. Both Checkpoint and Cisco Firewalls would offer high performance, deep packet inspection and fault-tolerance.

The Application Control Engine (ACE) modules are integrated into the Extranet Server Farm Switch Block at each site. These modules would provide server load-balancing and Secure Socket Layer (SSL) offloading. Just like the FWSM, the ACE module can also be virtualized and associated to FWSM contexts.

The virtualized contexts host a multitude of business applications, such as WEB, Transaction, Multimedia, Proxy Services, Employee Services, Partner/Vendor Services, Application Staging Services, Application Development Services, etc.

Intranet Secured Zone

The Intranet Secured Zone provides an additional layer of security and data integrity for internal server farms that provide public services. This zone would consist of Core Switch Blocks at each site connected via fault-tolerant high-speed gigabit (GigaMAN) circuits. These circuits would provide backend connectivity for data synchronization between sites, and network device management.
The FWSM and ACE modules are integrated within the E-Commerce Back-End Switch Block at each site. These modules would provide security, server load-balancing and Secure Socket Layer (SSL) offloading. The virtualized contexts host a multitude of internal business applications, such as Application Staging, Application Development, Database Services, etc.

Network Analysis Modules (NAM):

NAMs are integrated into the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block at each site. This NAM is a tool for Network Analysts that would identify application flows, protocol distribution, perform trend analysis, and capacity management. All collected data from these NAMs would be used to optimize application behavior, anomaly detection and isolate network problems.

Application Velocity System (AVS):

AVS appliances are connected to the Extranet Server Farm Switch Block and Intranet E-Commerce Back-End Switch Block at each site. This AVS appliance has a built-in application security firewall, which would identify and prevent application layer threats and data theft. These appliances provide acceleration, monitoring and securing web-based application delivery to all connected clients with out modifying clients or servers. The AVS appliance manages all client sessions by consolidating similar data sessions into a single session destined for the application server. So, all E-Commerce applications over HTTP or HTTPS are optimized with greater response time and reduced bandwidth requirements.

Intrusion Detection/Prevention System (ID/PS):

The Intrusion Detection/Prevention System consists of VPN/Security Management Solution (VMS); network intrusion detection sensors (NIDS); Host Intrusion Detection Sensors (HIDS); and [redacted]

VMS would provide security management capabilities to help meet the overall security needs. VMS also allows security analysts to manage and troubleshoot the configuration and the policies of NIDSs, HIDs, and firewalls.

The NIDS modules are integrated into the Internet Edge Distribution Switch Block, and the E-Commerce Back-End Switch Block at both sites. These NIDS modules would provide promiscuous inspection of network traffic, which would send an alert based on a signature-driven event. These events are also sent to the MARS for event correlation and validation.

The HIDS safeguards the entire server by preventing known and unknown malicious attacks such as Web defacement, buffer overflows, worms, newly discovered attacks, zero-day, etc. By blocking these attacks, the HIDS significantly decreases downtime and protects critical assets. The HIDS uses a combination of behavioral rules and signatures to prevent known and unknown attacks.

The [redacted][6] is an appliance-based solution that provides insight and control of the existing security deployment. The [redacted] allows the FTB to identify, manage, and counter security threats. It works with our existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution.

[redacted] transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. This threat mitigation appliance enables security analysts to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed within the EPI. This product supports log data from various security Hardware/Software solutions such as, vulnerability assessment tools, Antivirus, Windows 2000, and 2003 logs etc.

Summary

The new architecture and design presented in this solution would provide a high level of security with "zero-day" threat mitigation, geographical fault-tolerance, dual network paths and scalability for future growth.

Securing Franchise Tax Board's resources is the top priority of the EPI Project. The design details are sound and are composed of a complex labyrinth of security controls whose span extends from the Internet Public Access Zone to the Intranet Secured Zone. These controls are made up of dual-authored firewalls; an Intrusion Detection and Prevention System; Distributed Denial of Service Prevention System; and an Event Correlation System. This creates a highly secured transaction environment that is self-defending and that would protect the customer.

E-commerce infrastructure reliability is key to supporting a 24/7/365 uptime. The EPI Project, by design, accomplishes this by incorporating network redundancy across components, devices, and geographical sites. This methodology of redundancy promotes a self-healing environment that can prevent the loss revenue.

As FTB's participation in e-commerce grows and business requirements constantly change, the network infrastructure must have the ability to keep up. The EPI Project addresses this need by using a concept called "virtualization." Virtualization is the ability to create multiple environments on one infrastructure device or a group of devices. These environments allow a single device or group of devices to accommodate new e-commerce programs, so there's no need to purchase new equipment.

Many of the network devices used in this project support this concept and as a result, environments can be added or removed seamlessly. For example, the Extranet and Intranet Secured Zones host a set of secure environments. As new applications are created, new environments to accommodate these applications can be set up in a timely and cost effective manner.

[6] The [redacted] has been identified for costing purposes only since no product at this time can meet the proposed configurations. However, other products, including the current solution in place (ISS), will be evaluated to determine the most effective solution for FTB.

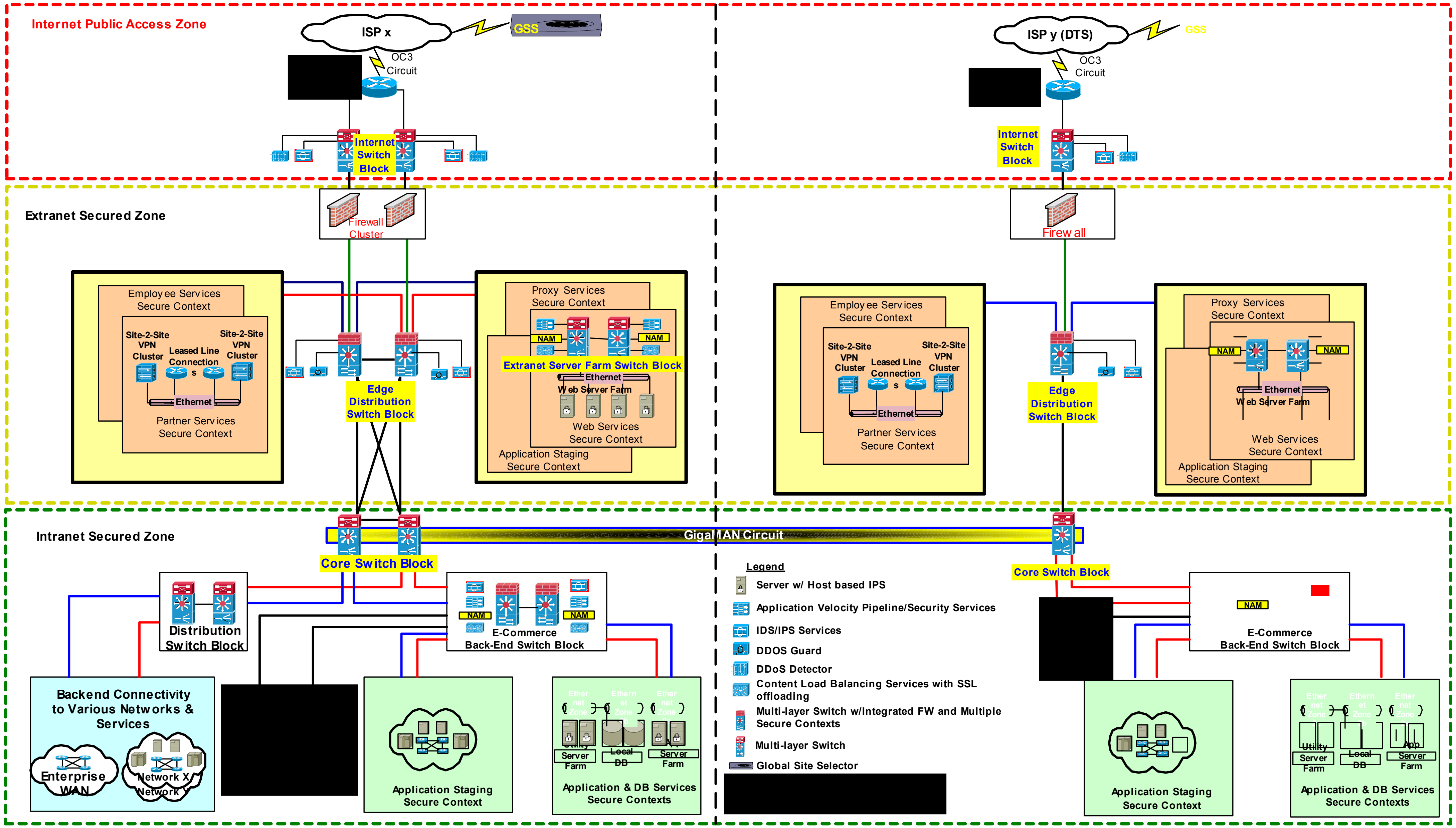
Advantages:

1. Two physical sites
2. Load balancing and redundancy
3. Would be able to leverage Department of Technology Services (Teale) physical site
4. Popular industry standard
5. Eliminates single points of failure from a network perspective, including facilities (Major fiber cuts, Electrical, etc)

Disadvantages:

1. Two separate sites: harder to manage
2. May require additional certifications of infrastructure to meet IRS requirements
3. Would require additional equipment, which equals added cost (Servers and Network equipment)
4. Interagency Agreement required
5. High cost to implement and support.

FTB E-Commerce Portal Infrastructure (EPI) Diagram 3



Revision 10 Date 11/07/2006

6.0 Project Management Plan

6.1 Project Manager Qualifications

The Project Manager for the E-Commerce Portal Infrastructure Project is a Data Processing Manager III in the Network Management Bureau at the Franchise Tax Board. He is the manager of the Enterprise Network Operations Section, which is responsible for managing all aspects of the E-Commerce Network that supports FTB's Internet applications. He has extensive knowledge of FTB's business and technology operations and has over eighteen years experience managing large infrastructure projects. Most recently, he was the project manager for the Phase III Voice and Data Infrastructure Project (#1730-167). The objective of this project was to provide the necessary voice and data infrastructure for FTB's new state office building. The project was completed successfully on time and under budget.

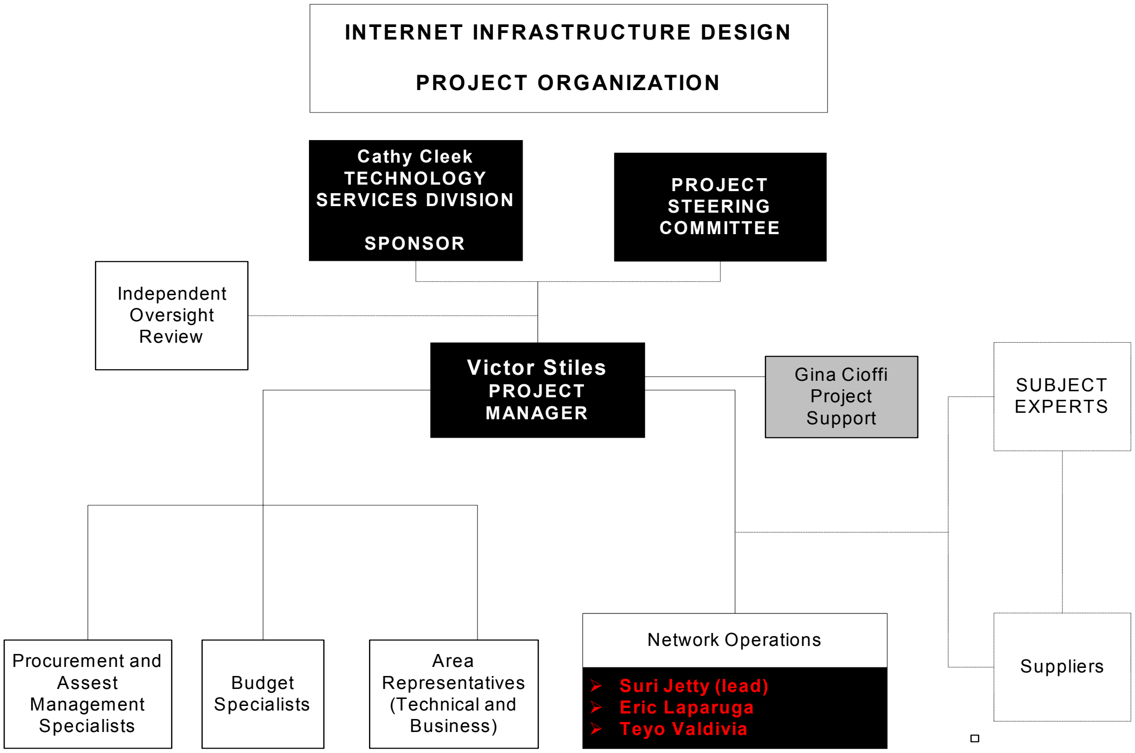
The Project Manager has an understanding of, and experience in: project planning; resource, cost and schedule estimating; project administration; budget management; risk assessment and management; identifying cost controlling opportunities, supervision and team building. He understands the concepts of organizational structure and is skilled at promoting communication between all participants. He has demonstrated an ability to direct and lead teams from varied technical and non-technical backgrounds. He has effective communication, problem solving and management resolution skills, and has developed an excellent working relationship with staff and all levels of management. In addition to extensive project management experience, the Project Manager has completed the Project Management Academy conducted by the Department of General Services.

Also see Appendix 1.

6.2 Project Management Methodology

The FTB project management methodology is based on *A Guide to the Project Management Body of Knowledge* (PMBOK) Third Edition; SIMM Section 45, Appendix A; and SIMM Section 200, *Project Management Methodology Guidelines*. For reportable projects, the Project Manager will, at a minimum, implement the required project management practices specified in SIMM 45.

6.3 Project Organization


INTERNET INFRASTRUCTURE DESIGN
PROJECT ORGANIZATION
Cathy Cleek
TECHNOLOGY SERVICES DIVISION
SPONSOR
PROJECT STEERING COMMITTEE
Independent Oversight Review
Victor Stiles
PROJECT MANAGER
Gina Cioffi
Project Support
SUBJECT EXPERTS
Procurement and Assest Management Specialists
Budget Specialists
Area Representatives (Technical and Business)
Network Operations
➢ Suri Jetty (lead)
➢ Eric Laparuga
➢ Teyo Valdivia
Suppliers

6.4 Project Priorities

Meaning of priority:

- Accepted: schedule or resources may expand, scope may be reduced.
- Constrained: no change in schedule, scope, or resources.
- Improved: minimize schedule or resources, maximize scope.

Schedule	Scope	Resources
Accepted	Improved	Constrained

6.5 Project Plan

During start up, the project manager will follow the standards of project management in PMBOK to develop the project plan. Microsoft Project will be used to develop the timeline and track the schedule, hours, resources, etc.

Resource needs will be defined during the development of the plan. It is anticipated that existing business and technical resources will be available to provide the support and expertise necessary to ensure successful implementation.

6.5.1 Project Scope

In Scope: EPI proposes to provide Internet network infrastructure and tools needed to effectively and efficiently manage, maintain and grow FTB's network platform. The infrastructure components of the EPI project primarily involve switches, routers, IDS (Intrusion Detection System), and PIX firewalls.

Out of Scope: This project does not provide e-application specific capacity, nor does it provide platform capacity for future applications.

6.5.2 Project Assumptions

- Funding will be approved timely by the Department of Finance.
- For the life of the project, management continues to recognize and support the need for the E-Commerce Portal Infrastructure.
- The business objectives and functional requirements are attainable.
- The necessary staff will be available to procure, install, test and implement the project.

6.5.3 Project Phasing

Project phases are not applicable to this project.

6.5.4 Roles and Responsibilities

Roles	Responsibilities
Project Sponsor	• Ensures that the project meets departmental, agency and state technology objectives prior to approval.

Roles	Responsibilities
	• Approves project feasibility study and implementation. • Ensures necessary resources are available. • Provides direction.
Project Steering Committee	• Reviews and approves change requests. • Resolves policy issues. • Reviews Quality control process results. • Provides and assigns staff for project. • Provides training resources if needed. • Reviews and approves risk management strategies. • Approves the proposed implementation schedule.
Project Manager	• Identify and resolve project issues • Provide status report to project sponsor, Steering Committee and Team Members • Manage project implementation • Evaluate and report project effectiveness • Approve all deliverable documents • Develop approach/recommendation to meet the business requirements, which includes the development of the new system and on-going maintenance thereafter • Identify personnel necessary to implement project • Manage project Risks • Facilitate communication with clients on all aspects of the project • Approve General System Design Documents and Detailed System Design Documents • Approve all Business Requirements
Project Support	• Provide support with writing FSR, project Scope, objectives, and deliverables. • Provide meeting facilitation support as requested by the Project Manager.
Project Team	• Manages and maintains project schedule. • Execute change & issue processes, quality assurance & control mechanisms, communication & risk mgmt plans. • Coordinates project efforts of all stakeholders. • Facilitates the development of the implementation schedule. • Executes the project implementation schedule.
Area Representatives (Technical and Business)	• Provide input to ensure that the Internet infrastructure design can meet FTB's business needs. • Collaborate with Project Team to develop implementation schedule. • Execute the implementation schedule. • Provide input to Quality Control process. • Control and track the inventory. • Provide performance measures to project team.
Procurement & Asset Management Section	• Purchases project hardware & software. • Addresses software license transfers.

Roles	Responsibilities
	- Acquires/maintains service contracts. - Coordinates procurement with the project team consistent with the implementation schedule.
Budget Support Staff	- Assists Project Team in managing, tracking, and reporting project costs.
POG Controller	- The project controller monitors the project's timelines and budget by ensuring project stays on track.
POG Analyst	- The POG analyst monitors the projects progress, and assists in the development, review and approval of required documentation.
Project Oversight Staff	- Provides project oversight and guidance

6.5.5 Project Schedule

#	Task	Start	Finish	Deliverable	Milestone
1.	Obtain GC Approval on FSR	5/08/06	5/30/06	FSR	FSR Approved
2.	Obtain Agency & DOF FSR Approval	6/01/06	1/12/07	FSR	FSR Approved
3.	Complete Information Technology Procurement Plan (ITPP) and obtain approval	5/09/06	1/30/07	ITPP	ITPP Approved
4.	Project Start	1/16/07			Begin Project Activity
5.	Research: Develop and release competitive bid solicitation(s) for Technical design Consultant(s)	1/17/07	3/16/07	Bid Documents ready for advertisement and distribution	Bid Documents Completed and sent to vendors
6.	Receive Technical Design Consultant Proposal	4/30/07	4/30/07		
7.	Evaluate and Review Technical Design Consultants Bid Response(s)	5/01/07	6/30/07	Bids Submitted	Bids received, reviewed and awardees selected
8.	Award (s) Technical Design Consultants bid	7/02/07	7/02/07	Prepare Agreement Documents	Agreement sent to Vendor(s)
9.	Technical Design Consultants Starts	7/16/07	10/01/07	Approved Contract	
10.	Prepare & Release Bid Documents for IV&V Oversight Services	1/16/07	2/28/07	Solicitation Document	
11.	Receive Vendor Proposals for Oversight Services	3/30/07	3/30/07	Vendor Proposals Documents	
12.	Evaluate/Review Vendor Proposals	4/03/07	4/30/07	Approved Evaluation & Selection Report	
13.	Award Oversight Vendor Agreement(s)	7/02/07	7/02/07	Prepare Agreement Documents	Agreement sent to Vendor(s)

#	Task	Start	Finish	Deliverable	Milestone
14.	Oversight Vendor Starts	7/16/07	7/16/07	Approved Contract	
15.	Begin the validation of Technical design, work with technical partners, and vendor partners - Prepare Component Infrastructure Bids	10/01/07	11/30/07	Design, parts list and FY 07/08 training request	
16.	Hardware Research: Develop and release competitive bid solicitation documents(s) for CMAS, and competitive bid acquisitions.	12/03/07	2/28/08	Bid Documents ready for advertisement and distribution	Bid documents completed and sent to vendors
17.	Software Research: Develop and release competitive bid solicitation document(s) for software license acquisitions.	12/03/07	2/28/08	Bid Documents ready for advertisement and distribution	Bid Documents Completed, sent to Vendors
18.	Research: Develop and release competitive bid solicitation(s) for Technical Implementation Consultant (s)	08/01/08	9/30/08	Bid Documents ready for advertisement and distribution	Bid Documents Completed and sent to vendors
19.	Receive/Evaluate/Review Bid Response(s) for Hardware	3/03/08	4/15/08	Bid(s) Submitted	Bids received, reviewed and Awardees selected
20.	Receive/Evaluate/Review Bid Response(s) for Software	3/03/08	4/15/08	Bid(s) Submitted	Bids received, reviewed and awardees selected
21.	Receive/Review Technical Implementation Consultants Bid Response(s)	11/17/08	12/17/08	Bids Submitted	Bids received, reviewed and awardees selected
22.	Award Procurement Hardware Agreement(s)	4/16/08	4/16/08	Prepare Agreement Documents	Agreement sent to Vendor(s)
23.	Award Procurement Software Agreement(s)	4/16/08	4/16/08	Prepare Agreement Documents	Agreement sent to Vendor(s)
24.	Award Technical Implementation Consultants Agreement(s)	12/18/08	12/18/08	Prepare Agreement Documents	Agreement sent to Vendor(s)
25.	Attend Technical Training	10/01/07	6/30/09	Technical Training	Technical Training Completed
26.	Received Hardware	6/16/08	6/16/08	Hardware	Hardware Received
27.	Received Software	6/16/08	6/16/08	Software	Software Received
28.	Technical Implementation Consultants Start	1/05/09	1/05/09	Approved Contract	
29.	Rack mount and patch Infrastructure	8/18/08	9/30/08	Equipment	Equipment

#	Task	Start	Finish	Deliverable	Milestone
	components (Hardware and Software)			installed	installed
30.	Burn-in equipment	8/18/08	09/30/08	Burn In	Acceptance of equipment
31.	Acceptance Testing	8/18/08	9/30/08	Hardware/Software Accepted	Hardware/Software Acceptance
32.	Configuration of Infrastructure Components	10/01/08	04/30/09	Components Installed	Installation Completed
33.	Develop Testing and Migration Plans	10/01/08	1/30/09	Documented testing and migration plans	Test and migration plans reviewed and communicated.
34.	Technical implementation Consultant on site to assist with migration (exact months TBD)	01/05/09	11/02/09	Implementation plan	Implementation
35.	Move servers and applications from existing DMZ to new EPI network (Implement testing and migration plans)	5/01/09	11/02/09	Infrastructure functions as expected	Project Complete – System Operational
36.	Conduct Project Retrospective	11/16/09	2/15/10	Lessons Learned document	Project Retrospective completed
37.	Prepare Post Implementation Evaluation Report (PIER)	6/01/10	11/02/10	PIER	PIER completed

6.6 Project Monitoring

The independent project oversight requirements specified in SIMM 45 will be followed; the oversight reviews will be consistent with the project criticality rating established by OTROS/Finance.

6.7 Project Quality

Technical staff from the Network Management Bureau (NMB) will work closely with the vendor through an acceptance-testing period to ensure that the products meet all project objectives and requirements.

6.8 Change Management

This project will use the standard FTB Change Control Process.

6.9 Authorization Required

This project requires approval by the Governance Council, the State and Consumer Services Agency, and the Department of Finance.

7.0 Risk Management Plan

7.1 Risk Management Approach

The risk management approach the Franchise Tax Board has developed to identify, analyze, respond to, monitor, and control project risk is based on *A Guide to the Project Management Body of Knowledge* (PMBOK) 2000, Chapter 11, issued by the Project Management Institute, and SIMM Section 45.

7.2 Risk Assessment Matrix

The high-level project risks are identified in the Risk Assessment Matrix. See Appendix 2.

7.3 Assessment

The high-level risk assessment is an initial broad view of the risk associated with the project. The identification of all potential risks uses the project work breakdown structure, project plan, and the PMBOK knowledge areas as input to the process.

7.3.1 Risk Identification

During the planning stage of the project, risk information is gathered in an initial meeting of the project manager and the project team members. Project staff is asked to bring a list of potential risk items to the meeting. The staff discussion of risks generates a complete list of potential risks.

7.3.2 Risk Analysis and Quantification

After identifying the potential risks, the project team reviews each risk to determine if it is tangible and measurable. Based on the analysis of each risk, the set of risks that will be formally managed are those deemed most likely to have a negative impact to the project.

7.3.3 Risk Prioritization (Severity)

The severity of a risk determines its priority and is based upon 1) potential impact of the risk on the project, 2) the probability of occurrence, 3) the risk mitigation timeframe and 4) risk exposure. The determination of risk severity is a qualitative assessment that takes into account both internal and external risk factors. At a minimum, the highest severity risks will be tracked in the project Risk Assessment Matrix.

7.4 Risk Response

The project team has identified the risk mitigation response to each of the risks listed in the project Risk Assessment Matrix. For each response that is accepted, a contingency plan has been developed and is summarized in the *Risk Mitigation and Contingency Plan* template for that risk.

7.5 Risk Tracking and Control

The objective of the Tracking and Control phase is to ensure that all steps of the risk management process are being followed and, as a result, risks are being mitigated. Risk tracking and control involves the oversight and tracking of risk mitigation action plan execution, contingency plan execution, re-assessment of risks, reporting risk status, and recording risk information changes in the project Risk Matrix.

7.5.1 Risk Tracking

The project manager is responsible for the high-level oversight of the execution of mitigation and contingency plans for all risks identified in the project Risk Assessment Matrix. The project manager is responsible for ensuring that the project sponsor is updated and approves of all changes in status for high-severity risks.

7.5.2 Risk Control

The project manager will re-assess the risk information in the project Risk Assessment Matrix to determine if any changes are needed. For example, the risk severity or timeframe could change based upon project events or other information. Re-assessment of risk information will be performed on a monthly basis; it may be performed more frequently if needed.

Risk status is included as part of the project status meetings. Risk status reporting will focus on high severity risks. Information presented will include the status of risk mitigation plans, changes in risk severity for known risks, and any new risks identified.

8.0 Economic Analysis Worksheets (EAWs)

See attached EAWs, Attachment 3.

List of Attachments

1. Executive Project Approval Transmittal
2. Project Summary Package
3. EAWs
4. Glossary
5. Appendix 1. Project Criticality Evaluation Factor
6. Appendix 2. Risk Assessment Matrix

Attachment 4 - Glossary

Access Control Server (ACS): Access Control Server provides authentication, authorization, and accounting (AAA—pronounced "triple A") services to EPI network devices that function as AAA clients, such as PIX Firewall, Switch, CSS, CE and router.

ATM: Asynchronous Transfer Mode. A network technology for local area networks, Metropolitan Area Network and wide area networks that supports real-time voice, video and data.

Cisco PIX Firewall: The Cisco PIX Firewall is a dedicated appliance based firewall. It provides secure access between an internal network and Internet, extranet, or intranet links.

Content Service Switch (CSS): The Cisco CSS Content Services Switches are Layer 4/7 aware, and provide front end for Web server farms and cache clusters.

Content Engine (CE): [redacted]

Data Link Control (DLC): DLC (data link control) is the service provided by the Data Link layer of function defined in the Open Systems Interconnection (OSI) model for network communication. The Data Link layer is responsible for providing reliable data transfer across one physical link (or telecommunications path) within the network.

DMZ: In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

Failover: Failover monitoring service works when there are two or more web servers running the same (or similar) web site. This effectively and safely keeps the site online - even if one of the web servers is down.

Fault Tolerant: Fault-tolerant describes a computer system or component designed so that, in the event that a component fails, a backup component or procedure can immediately take its place with no loss of service.

Fluke: A combination network monitoring and troubleshooting tool, including protocol analyzer. It also has cable-testing capabilities and RMON2 probe capabilities.

Gigabit Ethernet (GE): Networking protocol for connecting devices at 1000 megabits per second.

Hot Standby Routing Protocol (HSRP): Hot Standby Router Protocol (HSRP) is a routing protocol that allows host computers on the Internet to use multiple routers that act as a single virtual router, maintaining connectivity even if the first hop router fails, because other routers are on "hot standby" - ready to go.

IEEE 802.1Q: IEEE Standard relating to Virtual LANs (VLANs)

Intrusion Detection Response System (IDRS): IDS detects unauthorized activity traversing the network, such as attacks by hackers, and sends alarms to a management console with details of the detected event. The security or network administrator specifies the network traffic that must be inspected by the IDS.

Internet Service Provider (ISP): A company that provides customer access to the Internet

Layer 3 Switching (L3 Switching): Layer 3 switching technology that integrates routing with switching to yield very high routing throughput rates in the millions-of-packets- per-second range. The movement to Layer 3 switching is designed to address the downsides of the current generation of Layer 2 switches, which functionally are equivalent to bridges. These downsides for a large, flat network including being subjected to broadcast storms, spanning tree loops, and address limitations.

Local Area Network (LAN): A network that connects computers in a building or campus.

Metropolitan Area Network (MAN): A network that connects computers within a metropolitan area such as a city.

Network Analysis Module (NAM): The NAM collects data at all layers so network managers can obtain analyses used for fault-isolation and troubleshooting, capacity planning and management, performance-management, application monitoring, and debugging.

OSI (Open Systems Interconnection): OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network.

Protocol: In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are protocols between each of several functional layers and each corresponding layer at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard.
On the Internet, there are the TCP/IP protocols, consisting of:
Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level.
Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level.
Additional protocols that are usually packaged with a TCP/IP suite, including the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet.

Router: Network layer (Layer 3) device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information (occasionally called a gateway).

Stateful Failover: In which existing sessions should not be dropped

Stovepipe: Segmented infrastructure, which was implemented piecemeal.

Switch: Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer (Layer 2) of the Open Systems Interconnection (OSI) model.

Synchronous Optical Network (SONET): SONET is the American National Standards Institute standard for synchronous data transmission on optical media.

TACACS: This is an acronym for "Terminal Access Controller Access Control System". This is a type of authentication protocols that allow a network access server [redacted] to offload the user administration to a central server.

Token Ring: A token ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a binary digit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

VLAN: A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

Wide Area Network (WAN): A network in which computers are linked over a wide area.

Appendix 1 – Project Criticality Evaluation Factors – Reportable Projects

Factor	Rating	Substantiation of Rating
Size	Medium	One-time costs are $5,909,435 The estimated period from project approval to initial implementation is 34 months.
Project Manager	Low	Victor Stiles – Network Management Bureau 2005, Technical Project Manager, Enterprise-Wide Customer Service Platform II. Cost of project is $8 million. Current. 2003, Project Manager, Phase III Voice & Data Infrastructure Project. Cost of project is $7.1 million. Project lasts five years. 1998, Project Manager, Enterprise-Wide Customer Service Platform I. Cost of Project is $4.5 million. Project lasts less than 1 year.
Project Team	Low	Suri Jetty - Network Operations Section 2005, SSS III, Business Entities e-File Project (BEEF) and SWIFT/Tumbleweed Project 2004, SSS III, Firewall Replacement Project Cost of Project $600,000 Project Lasted one year 2003, SSS III, Centralized Authentication Project (CAP) and Child Support Automation Project (CCSAS) 2001, *SSS* III, Virtual Private Network project. Cost of project $317,408. Project lasts 2 years. 2000, SSS III, Network Backbone project that began in 2000. Cost of project is $4 million. Project lasts 5 years. 1999, SSS III, INC project Teyo Valdivia – Network Operations Section 2003, Technical Team Lead/SSSIII, Phase III Voice/Data Infrastructure Project, Cost of project is $7 million, Project lasts 2 years 2000, Technical Team Member/SSSII, Network Backbone Upgrade Project, Cost of project is $4 million, project lasts 5 years.
Project Type Elements	High	Component: Hardware *Activity Category:* Infrastructure *Element:* Network Operations Center
	Medium	Component: Software *Activity Category:* Infrastructure *Element:* Layered Product

(a) Factor		(b) Rating
1	Size	2
2	Project Manager	1
3	Project Team	1
4	Type	3
	Total:	7
	Average:	1.75
	Project Rating:	Medium

Appendix 2. EPI Risk Assessment Matrix

Risk ID#	**Risk Category**	**Risk Statement**	**Impact** Low Med High	**Probability** Low Med High	**Exposure** Low Med High	**Time Frame** Short Med Long	**Severity** Low Med High	**Mitigation Response** Eliminate Reduce Accept	**Risk Status**	Status Change Date
001	Technical	Staff training classes not available timely is very likely to delay implementation.	High	High	High	Long	High	Eliminate	Identified	
002	Technical	Migration may result in service interruption	Low	Medium	Medium	Long	Low	Eliminate	Identified	
003	Technical	Integrating Wiring Infrastructure may result in service interruption	Low	Low	Low	Long	Low	Eliminate	Identified	
004	Project Management	Date slippage due to resources constraints or equipment delivery delays is likely to cause project implementation delays.	Medium	Medium	Medium	Long	Medium	Eliminate	Identified	
005	Project Management	CMAS Procurement delays are likely to cause project implementation delays.	Medium	Medium	Medium	Long	Medium	Eliminate	Identified	

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

EXISTING SYSTEM/BASELINE COST WORKSHEET

All costs are shown in whole (unrounded) dollars.

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 20010/1	
	PYs	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Am**
Continuing Information Technology Costs										
Staff (salaries & benefits)	9.3	860,597	9.3	860,597	9.3	860,597	9.3	860,597	9.3	860
Hardware Lease/Maintenance		596,938		596,938		596,938		596,938		596
Software Maintenance/Licenses		97,328		97,328		97,328		97,328		97
Contract Services		0		0		0		0		
Data Center Services		0		0		0		0		
Agency Facilities		123,195		123,195		123,195		123,195		123
Other		20,199		20,199		20,199		20,199		20
Total IT Costs	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,**
Continuing Program Costs:										
Staff	0.0	0	0.0	0	0.0	0	0.0	0	0.0	
Other		0		0		0		0		
Total Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	
TOTAL EXISTING SYSTEM COSTS	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,257**	**9.3**	**1,698,**

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

PROPOSED ALTERNATIVE: Redesign Existing Network (3 Yrs. Financing)

All costs are shown in whole (unrounded) dollars.

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 20010/11	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs										
Staff (Salaries & Benefits)	0.8	71,921	5.5	532,638	9.0	852,549	3.2	299,672	0.0	0
Hardware Purchase		0		944,453		944,453		944,453		0
Software Purchase/License		0		74,777		74,777		74,777		0
Telecommunications		0		66,603		66,603		66,603		0
Contract Services										
Software Customization		0		0		0		0		0
Project Management		0		0		0		0		0
Project Oversight		0		0		0		0		0
IV&V Services		0		107,680		107,680		26,920		0
Other Contract Services		0		136,568		122,175		119,296		0
TOTAL Contract Services		0		244,248		229,855		146,216		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		1,647		91,964		96,910		84,316		0
Total One-time IT Costs	**0.8**	**73,568**	**5.5**	**1,954,683**	**9.0**	**2,265,147**	**3.2**	**1,616,037**	**0.0**	**0**
Continuing IT Project Costs										
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	7.5	685,539	11.2	1,028,308
Hardware Lease/Maintenance		0		0		216,242		216,242		216,242
Software Maintenance/Licenses		0		0		45,585		45,585		45,585
Telecommunications		0		0		123,195		123,195		123,195
Contract Services		0		0		0		0		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		0		0		0		16,291		24,436
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**385,022**	**7.5**	**1,086,852**	**11.2**	**1,437,766**
Total Project Costs	**0.8**	**73,568**	**5.5**	**1,954,683**	**9.0**	**2,650,169**	**10.7**	**2,702,889**	**11.2**	**1,437,766**
Continuing Existing Costs										
Information Technology Staff	9.1	839,176	8.8	812,624	7.9	730,372	2.6	243,457	0.0	0
Other IT Costs		837,171		836,564		834,618		277,023		0
Total Continuing Existing IT Costs	**9.1**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
Program Staff	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
Other Program Costs		0		0		0		0		0
Total Continuing Existing Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Continuing Existing Costs	**9.1**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
TOTAL ALTERNATIVE COSTS	**9.9**	**1,749,915**	**14.3**	**3,603,871**	**16.9**	**4,215,159**	**13.3**	**3,223,369**	**11.2**	**1,437,766**
INCREASED REVENUES		0		0		0		0		0

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

ALTERNATIVE (1): Dual ISPs - FTB In-House

All costs are shown in whole (unrounded) dollars.

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 20010/11	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs										
Staff (Salaries & Benefits)	0.8	71,921	5.4	536,185	8.9	856,096	3.1	302,231	0.0	0
Hardware Purchase		0		2,652,171		0		0		0
Software Purchase/License		0		209,986		0		0		0
Telecommunications		0		742,370		0		0		0
Contract Services										
Software Customization		0		0		0		0		0
Project Management		0		0		0		0		0
Project Oversight		0		0		0		0		0
IV&V Services		0		133,077		133,077		30,005		0
Other Contract Services		0		274,272		80,879		0		0
TOTAL Contract Services		0		407,349		213,956		30,005		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		1,647		134,535		119,349		6,827		0
Total One-time IT Costs	**0.8**	**73,568**	**5.4**	**4,682,596**	**8.9**	**1,189,401**	**3.1**	**339,063**	**0.0**	**0**
Continuing IT Project Costs										
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	7.5	688,406	11.3	1,032,609
Hardware Lease/Maintenance		0		0		216,242		216,242		216,242
Software Maintenance/Licenses		0		0		45,585		45,585		45,585
Telecommunications		0		0		615,046		615,046		615,046
Contract Services		0		0		0		0		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		0		0		0		16,363		24,545
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**876,873**	**7.5**	**1,581,642**	**11.3**	**1,934,027**
Total Project Costs	**0.8**	**73,568**	**5.4**	**4,682,596**	**8.9**	**2,066,274**	**10.6**	**1,920,705**	**11.3**	**1,934,027**
Continuing Existing Costs										
Information Technology Staff	9.3	839,176	8.8	812,624	7.9	730,372	2.6	243,457	0.0	0
Other IT Costs		837,171		836,564		834,618		277,023		0
Total Continuing Existing IT Costs	**9.3**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
Program Staff	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
Other Program Costs		0		0		0		0		0
Total Continuing Existing Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Continuing Existing Costs	**9.3**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
TOTAL ALTERNATIVE COSTS	**10.1**	**1,749,915**	**14.2**	**6,331,784**	**16.8**	**3,631,264**	**13.2**	**2,441,185**	**11.3**	**1,934,027**
INCREASED REVENUES		0		0		0		0		0

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

ALTERNATIVE (2): Dual ISPs - DTS and FTB

All costs are shown in whole (unrounded) dollars.

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 20010/11	
	PYs	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**
One-Time IT Project Costs										
Staff (Salaries & Benefits)	0.8	71,921	5.6	553,544	11.2	1,096,569	3.9	382,388	0.0	0
Hardware Purchase		0		3,847,678		0		0		0
Software Purchase/License		0		209,986		0		0		0
Telecommunications		0		1,050,531		0		0		0
Contract Services										
Software Customization		0		0		0		0		0
Project Management		0		0		0		0		0
Project Oversight		0		0		0		0		0
IV&V Services		0		176,823		176,823		40,275		0
Other Contract Services		0		358,272		116,879		0		0
TOTAL Contract Services		0		535,095		293,702		40,275		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		1,647		134,915		124,238		8,456		0
Total One-time IT Costs	**0.8**	**73,568**	**5.6**	**6,331,749**	**11.2**	**1,514,509**	**3.9**	**431,119**	**0.0**	**0**
Continuing IT Project Costs										
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	7.5	688,406	11.3	1,032,609
Hardware Lease/Maintenance		0		0		459,389		459,389		459,389
Software Maintenance/Licenses		0		0		45,585		45,585		45,585
Telecommunications		0		0		868,364		868,364		868,364
Contract Services		0		0		0		0		0
Data Center Services		0		0		0		0		0
Agency Facilities		0		0		0		0		0
Other		0		0		0		16,363		24,545
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**1,373,338**	**7.5**	**2,078,107**	**11.3**	**2,430,492**
Total Project Costs	**0.8**	**73,568**	**5.6**	**6,331,749**	**11.2**	**2,887,847**	**11.4**	**2,509,226**	**11.3**	**2,430,492**
Continuing Existing Costs										
Information Technology Staff	9.1	839,176	8.8	812,624	7.9	730,372	2.6	243,457	0.0	0
Other IT Costs		837,171		836,564		834,618		277,023		0
Total Continuing Existing IT Costs	**9.1**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
Program Staff	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
Other Program Costs		0		0		0		0		0
Total Continuing Existing Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Continuing Existing Costs	**9.1**	**1,676,347**	**8.8**	**1,649,188**	**7.9**	**1,564,990**	**2.6**	**520,480**	**0.0**	**0**
TOTAL ALTERNATIVE COSTS	**9.9**	**1,749,915**	**14.4**	**7,980,937**	**19.1**	**4,452,837**	**14.0**	**3,029,706**	**11.3**	**2,430,492**
INCREASED REVENUES		0		0		0		0		0

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

PROJECT FUNDING PLAN

All costs are shown in whole (unrounded) dollars

FSR EAW

	FY	2006/07	FY	2007/08	FY	2008/09	FY	2009/10	FY	200
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	
TOTAL PROJECT COSTS	**0.8**	**73,568**	**5.5**	**1,954,683**	**9.0**	**2,650,169**	**10.7**	**2,702,889**	**11.2**	**1,4**
RESOURCES TO BE REDIRECTED										
Staff	0.8	73,568	4.5	460,747	8.0	788,237	9.7	924,595	10.2	
Funds:										
Existing System		0		0		385,022		385,023		
Other Fund Sources		0		0		0		0		
TOTAL REDIRECTED RESOURCES	**0.8**	**73,568**	**4.5**	**460,747**	**8.0**	**1,173,259**	**9.7**	**1,309,618**	**10.2**	**1,3**
ADDITIONAL PROJECT FUNDING NEEDED										
One-Time Project Costs	0.0	0	1.0	1,493,936	1.0	1,476,910	0.3	1,337,425	0.0	
Continuing Project Costs	0.0	0	0.0	0	0.0	0	0.7	55,846	1.0	
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	**0.0**	**0**	**1.0**	**1,493,936**	**1.0**	**1,476,910**	**1.0**	**1,393,271**	**1.0**	
TOTAL PROJECT FUNDING	**0.8**	**73,568**	**5.5**	**1,954,683**	**9.0**	**2,650,169**	**10.7**	**2,702,889**	**11.2**	**1,4**
Difference: Funding - Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	

Total Estimated Cost Savings	0.0	0	0.0	0	0.0	0	0.0	0	0.0	

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

ADJUSTMENTS, SAVINGS AND REVENUES WORKSI
(DOF Use Only)

#

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 200	
Annual Project Adjustments	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**Amts**	**PYs**	**A**
One-time Costs										
Previous Year's Baseline	0.0	0	0.0	0	1.0	1,493,936	1.0	1,476,910	0.3	1
(A) Annual Augmentation /(Reduction)	**0.0**	**0**	**1.0**	**1,493,936**	**0.0**	**(17,026)**	**(0.7)**	**(139,485)**	**(0.3)**	**(1,3**
(B) Total One-Time Budget Actions	0.0	0	1.0	1,493,936	1.0	1,476,910	0.3	1,337,425	0.0	
Continuing Costs										
Previous Year's Baseline	0.0	0	0.0	0	0.0	0	0.0	0	0.7	
(C) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.7**	**55,846**	**0.3**	
(D) Total Continuing Budget Actions	0.0	0	0.0	0	0.0	0	0.7	55,846	1.0	
Total Annual Project Budget Augmentation /(Reduction) [A + C]	**0.0**	**0**	**1.0**	**1,493,936**	**0.0**	**(17,026)**	**0.0**	**(83,639)**	**0.0**	**(1,3**

[A, C] Excludes Redirected Resources

Total Additional Project Funds Needed [B + D]

Annual Savings/Revenue Adjustments

Cost Savings	0.0	0	0.0	0	0.0	0	0.0	0	0.0	
Increased Program Revenues		0		0		0		0		

Department: Franchise Tax Board
Project: EPI FSR (06-01)
Date: 11/09/06

ECONOMIC ANALYSIS SUMMARY

All costs are shown in whole (unrounded) dollars.

FSR EAW

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 20010/11	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
EXISTING SYSTEM										
Total IT Costs	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257
Total Program Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
Total Existing System Costs	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257	9.3	1,698,257
PROPOSED ALTERNATIVE	**PROPOSED ALTERNATIVE: Redesign Existing Network (3 Yrs. Financing)**									
Total Project Costs	0.8	73,568	5.5	1,954,683	9.0	2,650,169	10.7	2,702,889	11.2	1,437,766
Total Cont. Exist. Costs	9.1	1,676,347	8.8	1,649,188	7.9	1,564,990	2.6	520,480	0.0	0
Total Alternative Costs	9.9	1,749,915	14.3	3,603,871	16.9	4,215,159	13.3	3,223,369	11.2	1,437,766
COST SAVINGS/AVOIDANCES	(0.6)	(51,658)	(5.0)	(1,905,614)	(7.6)	(2,516,902)	(4.0)	(1,525,112)	(1.9)	260,491
Increased Revenues		0		0		0		0		0
Net (Cost) or Benefit	(0.6)	(51,658)	(5.0)	(1,905,614)	(7.6)	(2,516,902)	(4.0)	(1,525,112)	(1.9)	260,491
Cum. Net (Cost) or Benefit	(0.6)	(51,658)	(5.6)	(1,957,272)	(13.2)	(4,474,174)	(17.2)	(5,999,286)	(19.1)	(5,738,795)